User Perceptions of Security Risks in Multiple Authentications

by

Hervé Saint-Louis

A thesis submitted in conformity with the requirements
for the degree of degree of Doctor of Philosophy

Faculty of Information
University of Toronto

User Perceptions of Security Risks in Multiple Authentications

Hervé Saint-Louis

Doctor of Philosophy

Faculty of Information
University of Toronto

2018

Abstract

Authentication is an everyday practice in the information economy. When people use Facebook, Google, or Twitter to log in a third-party app they perform tertiary authentications. Authentication is often the only protection users have for personal information held by platforms and third parties. This personal information and the metadata produced by people has an exchange value for platform operators. This dissertation explores people's perceptions of security and confidentiality as they perform tertiary authentications and how platform operators benefit from data generated in the process.

The research design consisted of a 20-participants experiment and a policy analysis reviewing privacy and security policies of Facebook, Google, and Twitter answered these questions. What is the extent of the interplay between security and usability for platform operators that are commodifying from users' personal data through tertiary authentication; how are people managing and controlling their security and confidentiality as they perform tertiary authentications and what are the implications of those actions for users' perception of identity and privacy, and; which conditions and variables create a perception of false security in users performing tertiary authentications, and what factors of tertiary authentication affect users' sense of security? Through diagrammatic representations of their mental models and a questionnaire, the experiment measured how the test and control groups rated the value of their personal information after reviewing platform policies and how they managed their data when offered the chance to adjust their security and privacy settings before performing tertiary authentications.

Results show that while participants tried to secure their data, they were not as aware of commodification processes. Guided by the transactional token framework used to theorize the

process of commodification of people's personal information when performing authentication, the policy analysis explains how platform operators commodify users' data. This framework is a dialectic model that analyzes at once authentication and the monetization of attention while focusing on tertiary authentication. It unearths strategies used by platforms operators to collect users' information through their interaction with gamified security and privacy settings. It is argued that tertiary authentication which protects users' personal information sacrifices security for usability's sake. Security becomes a feature which people unknowingly interact with to provide more data to platform operators.

Acknowledgments

Remerciement à ma mère, Marie-Andréa Pierre qui prie pour moi chaque jour. Ce que femme veut, Dieu veut (des fois). Remerciement de Monsieur Picôt (Picoton) à mon feu père, Jean-Gérard Saint-Louis.

Je remercie les membres de mon comité de thèse doctorale, les Professeurs Rhonda McEwen, Brett Caraway, et Cosmin Munteanu.

Professeure McEwen, je vous remercie de m'avoir choisie comme votre premier doctorant. Ce fut un honneur. Je vous remercie de ne pas avoir eu peur de mon profil éclectique et de toujours été ma première ambassadrice. Vous m'avez tellement appris de chose et avez tenu votre promesse de faire de moi un chercheur hors pairs. J'ai beaucoup à apprendre mais je serai toujours reconnaissant de tout ce que vous avez fait et continuez de faire pour moi. Merci.

Professeur Caraway, vous m'avez promis un jour de m'amener à la ligne d'arrivée. Nous y sommes! L'exemple de votre profonde réflexion théoriques et votre support moral m'ont donné tellement de confidence et la volonté d'atteindre mon propre dessein. Merci.

Professeur Munteanu, vous avez prouvé maintes fois pourquoi j'étais l'étudiant et vous le mentor. Je n'ai aucune honte de dire que je demeure humble devant la vivacité de votre esprit et l'énergie que vous dédiez à votre travail et celui de tous vos étudiants. Merci.

À mes assistants de recherche, Abigail Baker-Bigauska, et Jameel De Leon, je vous dis merci. Abby, merci pour le dévouement que tu as portée à cette entreprise et pour l'exactitude de tes interventions. Jameel, je te remercie de l'énergie et de la curiosité que tu as eue. Ton enthousiasme a été très inspirant.

Chère Professeure Jacquelyn Burkell, je vous remercie de m'avoir donné un exemple de ténacité et de rigueur. Professeure Leslie Shade, je fais ma dance à la Snoopy grâce à vous!

Très cher Professeur Thomas Keenan, comme mon superviseur de maîtrise, vous n'avez jamais abandonné votre support et intérêt pour toutes mes démarches. Merci.

Cher Professeur Olivier St-Cyr, je vous remercie de m'avoir enseigné tant sur les statistiques, sur les théories des facteurs humains, que sur les interactions hommes-machines.

Il est important pour moi de souligner que sans l'encouragement et l'acharnement incroyable du Docteur Stéphane Guevremont, je ne me serais jamais inscrit à la maîtrise et ensuite au doctorat. Merci de toujours avoir cru en mon potentiel.

Comme nos ancêtres africains nous le rappellent, il faut un village pour former un enfant. Puisque que comme Marshall McLuhan l'a annoncé, nous vivons dans un village global, il nous faut de bons mentors pour former les professionnels de l'économie de l'information. Pour moi, ces mentors furent Luc Martin, ing., feu Pierre Antonini et feu Leanne Sanders.

Je remercie mes collègues Sandra Danilovic et Jack Jamieson.

Et à ma famille. Je remercie mon oncle Fritz Pierre, le premier chercheur de ma famille dont je n'ai pu citer dans ma recherche mais que je tiens à souligner ici. Ton livre (Pierre, Ayad and Jemai 1985), aussi rare qu'il soit, sur les services de santé gynécologique en Haïti est à l'Université de Toronto et je l'ai lu.

J'aimerais remercier mes sœurs Gaby, Igi, et Tatale. Ensuite, il y a Dédé qui pose tant de questions.

Je remercie mes amis qui m'ont aidé à poursuivre cette recherche. Merci Dayo, Alwish, Corina, et Spencer.

Finalement, ma formation n'aurait été complète sans l'apport ponctuel, de la Professeure Lynne Howarth, du Professeur Seamus Ross, du Professeur Matthew Ratto, de la Doyenne Wendy Duff, de la Professeure Jenna Hartel, de la Faculté de l'information, de la Professeure Tracey Bowen de l'Institut des communications, de la culture, de l'information et de la technologie, de la Professeure Dominique Scheffel-Dunand de l'Université York, du Professeur Robert Huebert, du Docteur Patrick Feng, du Professeur Terry Terriff de l'Université de Calgary, du Professeur Peter Hoffmann, et du feu Professeur Robert Vogel de l'Université McGill qui m'avait promis que je serais un jour très familier avec toute cette littérature.

Cette thèse est dédiée aux enfants que j'aurai, si Dieu le veut.

Résumé

L'authentification est une pratique quotidienne dans l'économie de l'information. Lorsque les utilisateurs utilisent Facebook, Google ou Twitter pour se connecter à une application tierce, ils effectuent des authentifications tertiaires. L'authentification est souvent la seule protection à la disposition des utilisateurs pour transmettre des informations personnelles détenues par les plates-formes et les tiers. Ces informations personnelles et les métadonnées produites par les personnes ont une valeur d'échange pour les opérateurs de plates-formes. Cette thèse explore les perceptions des gens en matière de sécurité et de confidentialité lorsqu'ils effectuent des authentifications tertiaires et la façon dont les opérateurs de plates-formes bénéficient des données générées durant le processus.

Une expérience avec 20 participants et une analyse portant sur les politiques de confidentialité et de sécurité de Facebook, Google et Twitter ont répondu à ces questions. Dans quelle mesure existe-t-il un compromis entre la sécurité et la convivialité des opérateurs de plates-formes qui profitent des utilisateurs grâce à une authentification tertiaire. Comment les personnes effectuent-elles des authentifications tertiaires lorsqu'elles gèrent et contrôlent leur sécurité et leur confidentialité? Quelles sont les implications de ces actions sur la perception l'identité et de la vie privée des utilisateurs? Quelles conditions et variables créent une perception de fausse sécurité chez les utilisateurs effectuant des authentifications tertiaires, et, quels sont les facteurs d'authentification tertiaire qui affectent le sentiment de sécurité des utilisateurs? Grâce à des représentations schématiques de leurs modèles mentaux et d'un questionnaire, l'expérience mesure comment les groupes de test et de contrôle ont évalué la valeur de leurs informations personnelles après avoir examiné les politiques de la plate-forme et comment ils ont géré leurs données lorsqu'ils ont la possibilité d'ajuster leurs paramètres de sécurité et de confidentialité avant d'effectuer des authentifications tertiaires.

L'expérience prouve que bien que les participants qui essaient de sécuriser leurs données, n'étaient pas autant conscients des processus de marchandisation. Guidé par le modèle de crédit transactionnel utilisé pour théoriser le processus de marchandisation des informations personnelles des personnes lors de l'authentification, l'analyse des politiques explique comment les opérateurs de plates-formes commercialisent les données des utilisateurs. Elle détermine les stratégies utilisées par les opérateurs de plates-formes pour collecter les informations des utilisateurs grâce à leur interaction avec la sécurité gamifiée et les paramètres de confidentialité.

On fait valoir que l'authentification tertiaire qui protège les informations personnelles des utilisateurs sacrifie la sécurité à des fins de convivialité. La sécurité devient une fonctionnalité dont les personnes interagissent sans le savoir pour fournir plus de données aux opérateurs de la plate-forme.

De necessitate est sapientia

Table of Contents

Acknowledgments iv

Table of Contents viii

List of Tables xiii

List of Figures xvii

List of Appendices xx

Chapter 1 Introduction 1

1.1 Motivation 1

1.2 Thesis Statement 2

1.3 Research Thesis 3

1.4 Background of the Study 4

1.4.1 Authentication and Risk 4

1.4.2 What Is a Platform? 7

1.5 Contribution 9

1.6 Structure of the Dissertation 10

Chapter 2 Literature Review 12

2.1 Perception, Risk, and Single-Sign-On 12

2.2 Human-Computer Interaction 15

2.3 History of Security through Interaction 19

2.4 Usable Security and Privacy 20

Chapter 3 Theoretical Framework 24

3.1 Forms of Authentication 25
3.2 The Transactional Token 28
3.2.1 Related Work 29
3.2.2 Approach 36
3.2.3 Discussion 38
3.3 Conclusion 80
3.4 Research Conjectures 80
Chapter 4 Research Approach 83
4.1 Research Design 84
4.1.1 Policy Analysis 84
4.1.2 User-Based Quasi-Experiment 87
4.2 Conclusion 100
Chapter 5 Findings – Experimental Results 101
5.1 Questionnaire Results 102
5.1.1 C2 Questionnaire Results 103
5.1.2 C3 Questionnaire Results 105
5.2 Qualitative Questionnaire Analysis 108
5.2.1 Open-Ended Questions Coding 110
5.3 Diagrammatic Mental Model Representations 115
5.3.1 Researcher-Produced Photographic Documentation 115
5.3.2 Participant Diagrammatic-Elicitation 118

5.4 Conclusion 152

Chapter 6 Findings – Policy Analysis 153

6.1 Introduction 153

6.2 Related Work 155

6.2.1 Privacy Policies 155

6.2.2 Developers' Policies 158

6.3 Approaches and Method 159

6.4 Technical Background & Analysis 160

6.5 Perceptual Evaluations of Policies 164

6.5.1 Facebook 165

6.5.2 Google 169

6.5.3 Twitter 172

6.5.4 Perceptual Evaluation Summary 175

6.5.5 Implications 176

6.6 Frame Analysis 177

6.6.1 Facebook's Data Policy 177

6.6.2 Google's Privacy Policies 183

6.6.3 Twitter's Privacy Policy 187

6.7 Transactional Token Analysis 189

6.7.1 Twitter 189

6.7.2 Facebook 192
6.7.3 Google 195
6.8 Conclusion 200
Chapter 7 Discussion 202
7.1 Research Question One: Background and Motivation 202
7.2 Research Question One: Answer 206
7.2.1 Technical Background Discussion 206
7.2.2 Perceptual Evaluation Discussion 208
7.2.3 Frame Analysis Discussion 212
7.2.4 Transactional Token Discussion 214
7.2.5 Research Question One Report 215
7.3 The Experimental Background and Motivation 221
7.3.1 Closed-Ended Answers 221
7.3.2 Conjecture 1: Mental and Design Models 225
7.4 Research Question Three: Answer 226
7.4.1 Limited Postings 227
7.4.2 Using Known Devices 227
7.4.3 Control over Place of Interaction 227
7.4.4 Password Management Practices. 228
7.4.5 Usability 229

7.4.6 Modalities and Sites of Interaction 229
7.4.7 Clone Clients 230
7.4.8 Tertiary Apps 232
7.4.9 Security and Privacy Settings 232
7.5 Research Question Two: Answer 233
Chapter 8 Conclusion 236
8.1 Contributions 236
8.1.1 Diagrammatic Representation of Mental Models and HCI Research 236
8.1.2 Transactional Token and Commodity Theory 237
8.1.3 Usable Security - Authentication and Privacy 238
8.1.4 Critical HCI 238
8.1.5 The Risk Society and Information Security 239
8.2 Future Research 239
References 241
Appendices 267

List of Tables

Table 1 - Forms of Authentication 27

Table 2 - Ephemeral Technology Model 48

Table 3 - Research Questions to Conjecture Mapping 82

Table 4 - Likert Scales 88

Table 5 - Experimental Road Map 90

Table 6 - Open-Ended Questions 94

Table 7 – Six Qualitative Themes 98

Table 8 - List of Questions Drawn from Themes 98

Table 9 - Closed Questions 102

Table 10 - Question 4 103

Table 11 - Question 7 104

Table 12 - Question 9 104

Table 13 - Question 10 104

Table 14 - Question 11 105

Table 15 - Question 1 106

Table 16 - Question 2 106

Table 17 - Question 3 106

Table 18 - Question 5 107

Table 19 - Question 6 107

Table 20 - Question 8 108

Table 21 - Diagrammatic-Elicitation Instructions 119

Table 22 - Qualitative Summary of Diagrammatic Representations Questions 122

Table 23 - Sample Qualitative Descriptions 123

Table 24 - Descriptive Summary of Diagrammatic Representations Metrics 123
Table 25 - Diagrammatic Complexity Scale 127
Table 26 - Participant 4 Diagram Complexity 127
Table 27 - Written Annotation Complexity Scale 130
Table 28 - List of Questions Drawn from Themes 132
Table 29 - Types of Coding Used 133
Table 30 - Disagreement Metrics 133
Table 31 - Logins Representation Details 138
Table 32 - Logouts Representation Details 139
Table 33 - Linear Path of Interaction: Detailed View 144
Table 34 - Twitter Labels 173
Table 35 - Alternate Conjecture 3 Testing Questions 223
Table 36 - Full List of Tasks and Conditions 267
Table 37 - Potential Participants' Self-Screening Survey 268
Table 38 - Participants Demographics 269
Table 39 - Experiment Protocols 270
Table 40 - Q1 Mann-Whitney Test 283
Table 41 - Q2 Mann-Whitney Test 284
Table 42 - Q3 Mann-Whitney Test 285
Table 43 – Q5 Mann-Whitney Test 286
Table 44 – Q6 Mann-Whitney Test 287
Table 45 – Q8 Mann-Whitney Test 288
Table 46 – Q4 Mann-Whitney Test 289
Table 47 – Q7 Mann-Whitney Test 290

Table 48 – Q9 Mann-Whitney Test 291
Table 49 - Q10 Mann-Whitney Test 292
Table 50 – Q11 Mann-Whitney Test 293
Table 51 - Latin Square 293
Table 52 - Types of Authentication 294
Table 53- File Name Protocol 298
Table 54- Shots per Participants 298
Table 55 – Coders' Profiles 299
Table 56 - Qualitative Summary of Participant's Diagrammatic Representations 299
Table 57 - Mental Models Summary 300
Table 58 - Is there a login? 302
Table 59 - Is there a logout? 303
Table 60 - Modalities of Interaction 304
Table 61 - Modalities of interaction on path 305
Table 62 - Primary / tertiary relationship 306
Table 63 - Reaction to access rights 307
Table 64 - Linear path 308
Table 65 - Model 309
Table 66 - Pairs 310
Table 67 - Preceding primary 311
Table 68 - Tertiary authentication and path 312
Table 69 - Differentiation 313
Table 70 - Initial site of interaction 314
Table 71 - Last site of interaction 316

Table 72- First Pass Qualitative Coding 317

Table 73 - Open Questions Second Pass Coding 323

List of Figures

Figure 1 - Marx's Commodity (Harvey, A Companion to Marx's Capital 2010, 26) 40

Figure 2 - Transactional Token - A Commodity 42

Figure 3 - Ephemeral Technology 47

Figure 4 - Private Property and Public Commons 50

Figure 5 - Expanded Private Property and Public Commons 60

Figure 6 - User Token Generation 63

Figure 7 - User License 67

Figure 8 - Authentication 69

Figure 9 - Targeting 75

Figure 10 - Data Exchange 75

Figure 11 - Third Parties and Advertisers 77

Figure 12 - Reconciliation 78

Figure 13 - Transactional Framework 79

Figure 14 - Magnetic Icon Chart 93

Figure 15 – P03 Sample Diagrammatic Representation 118

Figure 16 - High Number of Magnetic Icons Used (P10) 124

Figure 17 - Icons used as Logo (P18) 125

Figure 18 - Diagram without Magnetic Icon (P18) 126

Figure 19 – P04 Sample Diagrammatic Representation 127

Figure 20 - P14 Sample Diagrammatic Representation 128

Figure 21 – P04 Diagrammatic Annotations 128

Figure 22 – P07 Sample Diagrammatic Representation 130

Figure 23 – P01 Sample Diagrammatic Representation 131

Figure 24 - P18's dlvr.it Diagram 136
Figure 25 - P18's Hootsuite Diagram 136
Figure 26 - Modalities in Interaction Path (P01) 141
Figure 27 - P01 Nonlinear Path of Interaction Sample 144
Figure 28 - Example of Physical Mental Model from P19 145
Figure 29 - Example of Abstract Mental Model from P06 146
Figure 30 - P16's Paired Sample 147
Figure 31 - P10's Paired Sample 148
Figure 32 – P02 Primary Before Tertiary 148
Figure 33 - Tertiary Authentication Outside the Interaction Path (P01) 150
Figure 34 - Facebook for Playbook Tertiary Authentication (P09) 150
Figure 35 - Question 1 Likert Scale Results 283
Figure 36 - Question 2 Likert Scale Results 284
Figure 37 - Question 3 Likert Scale Results 285
Figure 38 - Question 5 Likert Scale Results 286
Figure 39 - Question 6 Likert Scale Results 287
Figure 40 - Question 8 Likert Scale Results 288
Figure 41 - Question 4 Likert Scale Results 289
Figure 42 - Question 7 Likert Scale Results 290
Figure 43 - Question 9 Likert Scale Results 291
Figure 44 - Question 10 Likert Scale Results 292
Figure 45 - Question 11 Likert Scale Results 293
Figure 46 - Recruitment Poster 295
Figure 47 - Consent Form Page 1 296

Figure 48 - Consent Form Page 2 297

List of Appendices

Table 36 - Full List of Tasks and Conditions 267

Table 37 - Potential Participants' Self-Screening Survey 268

Table 38 - Participants Demographics 269

Table 39 - Experiment Protocols 270

Figure 35 - Question 1 Likert Scale Results 283

Table 40 - Q1 Mann-Whitney Test 283

Figure 36 - Question 2 Likert Scale Results 284

Table 41 - Q2 Mann-Whitney Test 284

Figure 37 - Question 3 Likert Scale Results 285

Table 42 - Q3 Mann-Whitney Test 285

Figure 38 - Question 5 Likert Scale Results 286

Table 43 – Q5 Mann-Whitney Test 286

Figure 39 - Question 6 Likert Scale Results 287

Table 44 – Q6 Mann-Whitney Test 287

Figure 40 - Question 8 Likert Scale Results 288

Table 45 – Q8 Mann-Whitney Test 288

Figure 41 - Question 4 Likert Scale Results 289

Table 46 – Q4 Mann-Whitney Test 289

Figure 42 - Question 7 Likert Scale Results 290

Table 47 – Q7 Mann-Whitney Test 290

Figure 43 - Question 9 Likert Scale Results 291

Table 48 – Q9 Mann-Whitney Test 291

Figure 44 - Question 10 Likert Scale Results 292

Table 49 - Q10 Mann-Whitney Test 292
Figure 45 - Question 11 Likert Scale Results 293
Table 50 – Q11 Mann-Whitney Test 293
Table 51 - Latin Square 293
Table 52 - Types of Authentication 294
Figure 46 - Recruitment Poster 295
Figure 47 - Consent Form Page 1 296
Figure 48 - Consent Form Page 2 297
Table 53- File Name Protocol 298
Table 54- Shots per Participants 298
Table 55 – Coders' Profiles 299
Table 56 - Qualitative Summary of Participant's Diagrammatic Representations 299
Table 57 - Mental Models Summary 300
Table 58 - Is there a login? 302
Table 59 - Is there a logout? 303
Table 60 - Modalities of Interaction 304
Table 61 - Modalities of interaction on path 305
Table 62 - Primary / tertiary relationship 306
Table 63 - Reaction to access rights 307
Table 64 - Linear path 308
Table 65 - Model 309
Table 66 - Pairs 310
Table 67 - Preceding primary 311
Table 68 - Tertiary authentication and path 312

Table 69 - Differentiation 313

Table 70 - Initial site of interaction..... 314

Table 71 - Last site of interaction 316

Table 72- First Pass Qualitative Coding 317

Table 73 - Open Questions Second Pass Coding..... 323

Chapter 1
Introduction

This research project investigates how users perceive the security and confidentiality risks associated with the data they generate as they interact with apps and devices connected to the internet through authentication. This study is necessary because often, all that protects a person's online life is a password. The risk of a breech associated with tertiary authentication is compounded because both the primary account and its dependencies are affected.

In October 2015, hackers released a database from crowdfunding platform Patreon on the internet. The database included passwords, emails, people's names, messages exchanged between members, and their funding history. From this data dump, anyone can reconstruct the profile of various users and their interactions with Patreon up to September 24, 2015. (Godin 2015). This forced Patreon members to change their passwords and made all of their previous interactions public. The breach also potentially exposed the Facebook accounts of users who used the social network to log in Patreon. There is a possibility that the Patreon hack compromised the personal data of Facebook users who used the platform with the crowdfunding platform.

1.1 Motivation

If information security is as strong as its weakest link (Renaud 2003), securing a series of interactions between users and multiple devices, starting with authentication is fraught with risks. In this series of interaction between devices, apps and users, the latter are probably with whom problems occur. Operators design systems to perform under common scenarios. However, users are not common scenarios. It is my estimation that security mishaps most likely occur at the point where the user interacts with a technology.

This description of users as the weakest security link is not new. What this perspective recognizes is that information security as a risk is best controlled if operators who design and operate technologies focus on people first. This perspective drives the human-computer interaction (HCI) research area known as usable security. Usable security scholars investigate

issues related to how user interaction with technology affects their security. Broadly, this dissertation examines a classic usable security problem, which is the tension between usability and security.

There is a risk that when operators design highly usable and simple information systems for people to interact with, that security may be compromised to favour usability (Schultz, et al. 2001). Since security is about erecting barriers to control for undesirable user practices and errors[1], making technology usable often means removing limits meant to protect users. When securing an information system to protect users, there is a risk that the technology can become unusable for people. If technologies are unusable, users may try to circumvent security measures or avoid interacting with a technology entirely.

1.2 Thesis Statement

In this dissertation, using a Marxist-autonomist framework, I demonstrate the classic tension between security and usability when people perform multiple authentications with Facebook, Google, and Twitter. Profit-making goals of platform operators affect the design of third-party authentications. Authentication is less a means to secure people's information and profiles. Instead, it facilitates the exchange of user information and profiles with third-party apps that benefit platform operators. The findings from the research strongly suggest that the design of third-party authentications favours usability over the security and the confidentiality of user information and profiles. I prove this through an analysis of the commodification of third-party authentication promoted by Facebook, Google, and Twitter. I provide evidence for the argument that user interaction with the three platforms and some third-party apps through authentication

[1] A simple definition of errors is difficult. I consider two related approaches to the analysis and definition of errors. In Don Norman (1983, a)'s work, an error is a deviation from an intention. Intentions are intended actions to be executed (Norman 1983, a). An error in carrying out an intention, according to Norman is a slip (1983, a). An error in defining an intention is a mistake (Norman 1983, a). The second approach to error considers the response to errors and their origins. James Reason (Reason 2000) argues, errors can be classified as human flaws or as expected recurrent phenomenon that can be minimized through system designs. R. Amalberti (2001) describes these two approaches as being part of one continuum where at first researchers attempted to understand the origins of errors and then, how to prevent them.

has a transactional value that benefits platform operators. This theoretical explanation adds a missing understanding of processes of commodification occurring with online platforms.

Similarly, I argue that people using the three selected platforms are unaware of how the commodification of third-party authentication can affect their security and confidentiality. Through the policy analysis, I discovered that third-party authentication as used by platform operators favours usability over security. Using a quasi-experiment and a questionnaire, I demonstrate how users perceive their security and confidentiality when performing multiple authentications using Facebook, Google, and Twitter. Finally, I measure participants' awareness of the implications of exchanging their personal information through multiple authentications to gain access to features.

1.3 Research Thesis

This study explores usable security risks of primary systems and tertiary authentications. I am interested in understanding how users make sense of security and risks when performing tertiary authentications. My initial position is that platform operators rely on security practices like tertiary authentication to protect users because it benefits their own profit-making objectives. Tertiary authentication is one measure through which platform operators transform users' information into profit-making objects. This study investigates the transformation of users' personal information into profit-making objects through tertiary authentication and explores users' perception of that process through three research questions (RQ).

a) (RQ1) What is the extent of the interplay between security and usability for platform operators that are commodifying from users' personal data through tertiary authentication?
b) (RQ2) How are people managing and controlling their security and confidentiality as they perform tertiary authentications and what are the implications of those actions for users' perception of identity and privacy?
c) (RQ3) Which conditions and variables create a perception of false security in users performing tertiary authentications, and what factors of tertiary authentication affect users' sense of security?

Some of the third-party products and services that require users to perform tertiary authentications are not always vetted by platform operators. The third-party plug-in world is large and varied. While platform operators often dismiss rogue third parties, many cases can be nebulous. Potential rogue third parties may not be monitored sufficiently and detected before they can be a risk to users. Once information about a user has been transferred from a platform to a third party, this information is theirs. Users must count on the goodwill of third parties with their personal confidential information after transfer. Other risks such as viruses, Trojans horses, continue to be threats with third-party apps. Users are the ones deciding to allow and proceed with tertiary authentications. Therefore, analyzing how users perceive tertiary authentication matters.

1.4 Background of the Study

So far, the terms risk, authentication, and platform have appeared abundantly in this introductory chapter without proper definitions. To provide more insight into the stakes of the problem space this dissertation is tackling, I will define and explain some of the background related to risk, authentication, and platform that shape this study. My understanding of risk borrows from post-modern social theory adding information security as, yet another risk people must confront every day. While my basic definition of authentication borrows from computer science and usable security literatures, in this dissertation I offer theoretical and philosophical examination of authentication as part of this study's theoretical framework. The definition below sets the stage for a more profound exploration of authentication as an everyday practice in the information economy. While the term platform seems evident, as will be seen below, it is a term that has many usages. More importantly, I want to clearly explain what a platform is and what it is not, in the context of this study.

1.4.1 Authentication and Risk

Risks are fears humans perceive about potential negative outcomes and lack of control over man-made changes to their living environment (Beck 2000). Spam, online fraud, viruses, Trojan horses and worms are types of information security risks that people worry about just like environmental collapses, health epidemics, and economic mayhem. Yet, these data-integrity risks are not the only ones associated with information security. Passwords, a form of authentication,

are often the only online security processes that users interact with. How users perceive security enabled by authentication as they interact with technology is another form of information security risk. For example, when a Facebook user worries about sharing personal information to interact with others and have access to more of the social network's features, she may perceive that interactions come at a personal cost to her sense of privacy.

To prevent most information security risks, the service providers whose role is to develop and commercialize Facebook, Google and Twitter, ask users to log in (i.e., to authenticate) their identities before interacting with information hubs. These information hubs, or platforms, manage the exchange of information between users, third-party apps, stationary and mobile devices, such as desktop computers, smartphones, watches, tablets, and even cars. Are log ins enough to alleviate the perceived risks that people have when using these web-based platforms, particularly when users may perceive authentication as a cost? While there are other processes to prevent information security risks, such as encryption, for platform operators, authentication remains the preferred prevention practice. In this study, we find out how users feel about multiple authentications.

Authentication has become an important practice for how users interact with technology. While operators can collect confidential data about their users even when they do not login onto their platforms, authentication confirms the identity of a person. When a user has performed an authentication, a barrier has been removed in the continuing interaction with information systems. Though users may perceive themselves as safer for being authenticated, with third-party authentication, there may be more ubiquitous opportunities for platform operators to collect confidential data from users. Users are increasingly faced with opportunities to use a platform and its third-party's products and services. In exchange for this increased access, they must divulge part of themselves to platform operators. Operators commodify this divulged information with third parties. The increasing sharing of more confidential information becomes the cost of entry and access to a platform.

Philosophically, the act of authentication is about determining truth. The truth sought is the identity of the person allowed to access an information system, like an app, a platform, or a device. Authentication is a form of interaction between a person and a technology. There are two

parts to authentication. The first is about the verification of a user's identity (Chiasson and Biddle 2007). The second part is the authorization users get to use and access resources within an information system (Chiasson and Biddle 2007). Passwords, tokens, biometrics and federated single sign-on (Bonneau, et al. 2012) are some of the many forms of authentications used. My position on authentication is that it is a transaction between a user and an information system where the sharing of one's identity becomes the cost of accessing a platform such as a social network.

While platform operators want to protect users' information to avoid costly class actions lawsuits, such as in the Patreon case, a user's personal information obtained through a transaction such as an authentication has a value as a commodity. This commodity can be sold to advertisers and other third parties such as financial institutions including banks, credit rating agencies, or governments, and health or revenue departments who value having an insight into the profile and behaviour of a potential customer, a survey respondent, or even a patient. This commercialization of user's information exchanged against access to a service or platform is a contemporary form of commodification (Moulier Boutang 2008).

Users' information is at the mercy of operators' security and confidentiality protections mechanisms. Confidentiality differs from privacy. I define confidentiality as the protection of documented user information held in confidence through technology.[2] For example, Facebook asks its users to navigate and understand ever-changing and often complex security mechanisms. These corporate mechanisms, I argue, pit the confidentiality of users' information against the commodification desired by platform operators. Users' personal information as commodities have commercial values. Technology start-ups often push privacy boundaries through technology innovation and exploratory marketing practices (Rubinstein and Good 2012).

Users interact with platforms in their personal and public lives. For example, they may bring their personal smartphones to work, or a company assigned tablet home. Apps such as

[2] Inspired by Marshall McLuhan (1994), I broadly define technology as an extension of human senses. A filing cabinet, as well as a desktop folder are both methods to classify and organize documents. I further define and compare privacy and confidentiality in Chapter Two (Literature Review).

Facebook, Gmail (Google), and Twitter may be installed in both their personal and work-related devices. Some apps such as Dropbox, Microsoft Office 365, or LinkedIn may manage the exchange of information between personal and professional aspects of users' lives. Many of these apps interact with one another and with third-party apps. The main means of interaction for users across multiple platforms, plug-ins and devices is authentication. Increasingly, to use many third-party plug-ins (or apps) users must first log in a main platform. Authentications verify the identity of users and allow information to be transferred elsewhere. Similarly, many third-party app operators require users to register new accounts through the authentication of their existing profiles from original platforms.

1.4.2 What Is a Platform?

In the context of this study, platforms are computational spaces that are software-based where users and third-parties interact. This definition borrows from Tarleton Gillespie (2010) who identifies several traditional definitions for platforms but excludes purely hardware-based and operating systems. They can be computational infrastructures that support the development and exploitation of information systems; they are also elevated architectural spaces upon which people and things stand on; they can be figurative spaces that refer to the foundational place that allows people and ideas to be built upon; finally, platforms can be political products that frame the agenda of political actors in societies (Gillespie 2010).

I define platforms that share information and authentication with tertiary ones as primary systems. The primary system, in this context, would be platforms such as Facebook, or LinkedIn. A tertiary system is a third-party service that uses user information originating from a primary platform. An example of a tertiary app is Talon, a Twitter client for Apple's iOS mobile operating system. The BlackBerry Facebook client built and operated by BlackBerry on its mobile devices is also a tertiary app. In both cases, each app retrieves users' complete information and performs operations as standbys apps where official apps from Twitter and Facebook are not available. To replace existing clients of platforms such a Twitter and Facebook with third-party clones, users must enable the tertiary apps to use a primary system.

Between primary and tertiary authentication, there is also secondary authentication. Primary platform operators operate apps that perform secondary authentications. However, user data exchanges between primary and secondary is through authentication. Although YouTube could originally have been considered as an independent primary platform, with the integration of Google accounts into the video-sharing app, it has become a service that relies on secondary authentication. Users' profiles are retrieved from a central Google database used for other Google services such as Google+, Docs, and Gmail.

Apps like Facebook, Google's Picasa, LinkedIn, and Twitter, let users access third-party services by reusing their account profiles. To access third-party services, the apps let users reuse their existing authentications. The purpose of this mechanism is to facilitate users' access to external services, reduce the number of profiles created and to exchange data between systems. This mode of interaction design favours a safer user experience. Log in with passwords allows users to modify data contained within these apps. Often, without platform authentication, users are limited to browsing and searching information from networked services. Chapter 3 defines primary, secondary, and tertiary authentication in more detail.

A platform is not an operating system. An operating system is software (a logical layer) that manages hardware (physical systems) (Newman 2010). Just like platforms, operating systems accommodate third-party apps. However, operating systems are multifunction software that manage more than one type of operation. For example, while managing user accounts through authentication, they also manage the stability and security of users' devices. They perform connections with various peripheral devices through ports, such as USB keys, printers, computer mice or screens.

Platforms, on the other hand, are specialized software that manage user profiles to enable them to perform set operations. Authentication becomes the main way platforms allow users to interact with them. Platforms have increased their reach and offering, which is why they welcome third-party apps. Recent operating systems, such as Android 5, iOS 9 and Windows 10 are also focusing more on the commodification of their users by making authentication an important interaction prerequisite. Yet, operating systems must still manage radio signals, drive space, and file management. Platforms can operate as supplementary logical layers on top of

operating systems. Platforms are, therefore, clients of operating systems that may hide the operating system layer interaction from users. Operating systems are always tied with one physical device, even when they communicate and transfer information to other devices and operating systems through authentication platforms can operate from any user device. Primary authentication allows users to interact with platforms on multiple devices at once.

1.5 Contribution

As a human-computer interaction (HCI) researcher, my field of interest is usable security. I pursue research in usable security as a social scientist. Social sciences have proven relevant in responding to HCI problems usually answered by human factors/ergonomics, computer sciences, psychology and industrial design. Information systems and information studies originate from the social sciences.

While information systems is an applied discipline from management (Grudin 2012), information studies investigate issues larger than the enterprise. Information studies started as an applied social science with a strong technical core comprised of library science and information science. Prior to the 1960s, library science grew from a clerical practice of classification, and document retrieval (Van Fleet and Wallace 2002, 105), into a professional service in support of users (Day 2001, 31). Information science was a reformulation of various European and American traditions from the field of documentation (Van Fleet and Wallace 2002, 104) (Rayward 1983, 351-353). The polarization of scientific and humanistic traditions within library and information sciences favoured a positioning towards information studies, as a middle-ground rooted in social sciences (Bonnici, Subramaniam and Burnett 2009, 264).

As a discipline, information studies has always focused on serving patrons rather than forcing them to adapt to a technology. This is an important distinction from information systems whose prime beneficiaries were industry and the corporation. User studies is one example where information scholars shifted toward social sciences. Information scholar Tom Wilson (2000, 51) argues that until the mid-1970s, most research in information studies was focused with information systems rather than users. He adds that most user studies at the time were about how

people used systems and the needs they had to satisfy as opposed to studying users and their interactions with information (T. D. Wilson 1994).

Librarians and information scholars dedicate their efforts to improving the work of the individual, not the organization, nor technology. My contribution to usable security is informed by user focus and advocacy stemming from information studies. While I am myself a human-computer interaction scholar, critical theory topics such as the commodification of information for profit-seeking by large platform operators are of interests to me. An important contribution of this research is the operationalization of social theory and critical approaches that are familiar to social scientists but seldom to their computer science colleagues. The main shape of this operationalization is through the fulfillment of a quasi-experiment flavoured with insights from critical theory and phenomenology.

A second important influence in my research comes from my professional background as a cartoonist. This has influenced my preference for laying out my theoretical model using visual means and to seek insight into the mental models of the participants of this study. This personal motivation led me to craft an original and detailed research method through diagrams that allow HCI researchers to confidently peruse the mental models of participants involved in research projects. This method is flexible and addresses several flaws found in previous mental model research methods used by HCI scholars.

I introduce critical theory approaches to the study of human computer interaction, expanding the discreet approach of HCI. I demonstrate how this discipline can answer macro-level questions usually seen as the strength of communications and science and technology studies. I use experimental methods in the context of HCI to test social theories, like Manuel Castells (2012) did with network studies and sociology. Another important contribution is a brief history of the information security using human-computer interaction perspectives.

1.6 Structure of the Dissertation

Seven chapters follow. Chapter 2 is a literature review that expands on concepts briefly introduced above such as the literature on information security, HCI, and usable security. It also explores the critical literature from communications and media studies that inform the critical

outlook adopted in the analysis. Chapter 3 expands on the theoretical framework which combines an understanding from HCI and critical studies literature introduced in Chapter 2. The theoretical framework chapter explains the transactional token model and adds depth to the tertiary authentication notion briefly covered in the introduction. At the end of Chapter 3, I present three conjectures which allow me to operationalize the research questions from the introductory chapter. Chapter 4 explains the research design and research methods necessary to perform analyses that will allow me to answer the research question. The research design features two sets of methods that answer parts of the research's questions. The first set of research methods analyse the user-side of the tertiary authentication through an experiment where a test and control group were queried about their mental models. The findings for the quasi-experiment which includes a user-based questionnaire are explained in Chapter 5, Findings – Experimental Results. The second set of research methods help me perform a policy analysis of platform operators' security and privacy documents. This part of the study allows me to understand the extent of the commodification of users' personal information as they perform tertiary authentications. The findings for this part of the research are covered in Chapter 6 under Findings – Policy Analysis. Chapter 7, Discussion makes sense of the findings from Chapter 5 and Chapter 6 to determine if the research questions and their supporting conjectures were verified. Finally, Chapter 8 offers a conclusion based on the discussion and offers future avenues of research based on the work presented in this dissertation.

In the next chapter, the Literature Review, I appraise the relevant literature from the discipline of HCI and begin to operationalize people's perceptions of security using technology. Research from the last decades has expanded usability's reach to consider other aspects that affect how users interact with technology in their everyday practices beyond instrumental, and behaviourists' approaches. This expanded view of usability considers the context that surrounds the user such as his environment, cognitive, and experiential considerations. This expanded view of usability is user experience. User experience borrows philosophically from phenomenology (Hassenzahl 2008). Through this literature, I seek to explore and frame interaction as a practice at the core of all exchanges between people, between technologies, and between people and technologies.

Chapter 2
Literature Review

To answer questions about users' perceptions of security risks in tertiary authentication, I draw on human-computer interaction including the work of Paul Dourish and Don Norman. Based on Dourish's embodied interaction theory of human-computer interaction, I sketch analogies to the history of information security through user interactions. Jeffrey R. Yost's account of computer security is the backdrop from which I weave a history of security through interaction. Since perceptions are based on preconceived ideas held by humans who interact with technology, I build on Don Norman's adaptation of mental models' theory for HCI to define perceptions in the context of usability and human-computer interaction. Finally, I survey the literature on usable security to help identify gaps commonly found in information security research. For example, one important gap identified in the usable security literature is research that covers both authentication and privacy in the same study. This is a gap that this dissertation seeks to fill.

Information security research often acknowledges the importance of the user in security measures. However, users are not often the core security concern of information security experts (Schultz, et al. 2001). I position my approach to user studies by referring to the literature on user experience. Before proceeding, I will review some of the work related to the problem of tertiary authentication and people's perception of security, privacy and confidentiality risks, when using such processes.

To achieve this, I review some of the early literature from usable security about users' perceptions of security. Some of this work (Adams and Sasse 1999; Dourish, Grinter, et al. 2004) helped shift the blame away from users to encourage developers and organizations' security administrators to enable their information systems to be usable to gain support and acceptance from users. Today, such suggestion seems obvious, but it was not even a decade ago.

2.1 Perception, Risk, and Single-Sign-On

Anne Adams and Angela Sasse's "Users Are Not the Enemy" (1999) is an important foundational research for understanding people's perceptions of security. In this classic usable security article, Adams and Sasse surveyed participants about their authentication practices while

considering the organizational context that affected respondents' choices and actions (1999). They found that participants had poor understandings of security practices (Adams and Sasse 1999). Authentication processes mandated by organizations would often force users to circumvent security processes that were incompatible with work practices or prevented them from performing their duties (Adams and Sasse 1999). Because organizations did not share much information about security risks with respondents, users lack the appropriate knowledge and sensitivity (Adams and Sasse 1999). In turn, organizations reacted by treating users as enemies that had to be managed and contained for their own good (Adams and Sasse 1999). This study, while not the first to advocate user-centric security and authentication practices, contributed necessary research data by surveying many end-users and inquiring about their perceptions of security measures and authentication.

Dourish et al. (2004) explore users' security practices with ubiquitous computing and the challenges that mobile technologies create. While much of the study focuses on adapting usable security to the mobile and ubiquitous domain, the article offers invaluable insights about the strategies users employ to mitigate the management of their security. For example, they may delegate the management of their security to knowledgeable individuals, or organizations (Dourish, Grinter, et al. 2004). Dourish et al. hint that these strategies are the results of existing perceptions and user's experience of security (2004). While not as relevant today because of technological changes and how users interact with ubiquitous and mobile technologies the article offers the kind of qualitative assessment that is used in my research project.

American philosopher Charles Sanders Peirce first posited the idea of mental models (Johnson-Laird, Mental Models and Cognitive Change 2013) but it was Kenneth Craik (Craik 2010) who developed the concept using philosophical approaches to delineate a cognitive theory based on how humans reasoned. Craik was an early cognitive psychology researcher trained as a philosopher who wrote the seminal work on mental models, a theory of how people think things work.

Psychologist Philip Johnson-Laird (2013) contributed the theoretical and experimental foundation of mental models' research which usability and user experience researcher Don Norman (2013), introduced to HCI. The definition of mental models chosen by Norman adheres

to cognitive science perspectives. According to Johnson-Laird (2010), mental models are shortcuts humans create from the perceptions they have derived from the world to lessen their cognitive load and reliance on reasoning to solve everyday problems.

While researchers (Kline, He and Yalaciecegi 2011; Garg and Camp 2014) rely on user-surveys to evaluate perceptions of security risks, their approach has been vastly different even in related disciplines like HCI and social informatics. Garg and Camp attempt to explore respondents' mental models although there are scant details about how they assessed mental models. Neither Kline et al. nor Garg and Camp framed their risk framework on Beck's (2000)social theory as I do in this study.

Using a series of questionnaires to query participants, Kline et al. (2011) observed that respondents in one study based their assessment of security of websites on soft authentication metrics, such as site reputation and peer trust rather than relying on technical authentication metrics such as digital security certificates. Garg and Camp (2014) explore mental models and respondents' perceptions of security risks. Their study focuses on analyzing how different types of risks (medical, criminal, physical, warfare, and economic) are communicated and perceived by users (Garg and Camp 2014). Based on an assessment of participants' responses, they suggest communication strategies based on people's mental models about risks. While their usable security work features in the background of their research, they do not concentrate on the usability of risk communication.

Sun et al. (2013) produced a complementary study to this research project when they investigated users' perceptions of single-sign-on (SSO) protocols. The researchers tested users' perceptions and interactions with SSO protocols and then performed iterative tests on new proposed SSO implementations. Their study also measured users' mental models to identify respondents' conceptual gaps in their understandings of SSO. A major difference in their study design and the one in this research project is the use of SSO schemes as the initial site of interaction where users then navigate to a third-party site. All authentications are kept in a central repository and used as needed when accessing a tertiary resource. This differs from the aim of the work performed in this dissertation which as well as exploring the commodification of

people's personal information, also treats tertiary authentication as a distinct type of SSO where the user accesses the third-party site of interaction before choosing an authentication mechanism.

Details about the metrics used to infer meaning to the representation of respondents' mental models by Sun et al., are scant, and based on quantitative analyses alone. Moreover, the authors frequently describe participants' mental models as being incorrect because of their divergence with design models. Mental models are never incorrect. They reflect people's understanding in the moment. They are not meant to reflect design models accurately. Little understanding of users' mental models is possible if they are subsequently classified as flawed by researchers.

The use of people's data by platform operators is occurring and may become an established practice. For example, Carrascal et al. (2013) and Staiano et al. (2014) have performed experiments where users were compensated based on the level of disclosure of personal and confidential information with online platforms with identity-compensating marketplaces. Although these studies did not research users' perception of security through authentication, the models they proposed for telecom operators will probably be adopted by the industry. Both Verizon and Bell Canada have announced in recent years policies to use their subscribers' usage data without seeking their agreements for profit (Rosen 2012; CBC News 2013).

2.2 Human-Computer Interaction

Human-computer interaction (HCI) literature often refers to user experience epistemologically as an enhanced form of usability (Sauro and Lewis 2012; Norman 2013; Tullis and Albert 2013) or as a subset of usability (Weir, et al. 2010). However, borrowing from Marc Hassenzahl (2008) I frame user experience as a concept grounded within phenomenology. As I use a phenomenology-based conceptualization of user experience, I investigate the work of researchers that have differentiated user experience from usability. The research that I refer to borrows from social theory and qualitative evaluations. This allows me to recall similar work done outside of user experience in other areas of HCI. Just like user experience, ethnomethodological approaches to HCI refer to social theory and phenomenology.

Through this journey the literature on human-computer interaction, commodity theories, identity philosophy, usable security, usability, user experience, and ethnomethodology, I frame questions about how users' perceptions of security differ from the traditional conceptual security theories and practices used in the information security world.

The HCI literature is worth considering when looking at user perceptions. HCI scholar Paul Dourish (2001) explains the history of human-computer interaction as perceptual relationships at first materially embodied, then moving to more abstract forms of perception and interactions, and finally reaching out again for the material. Dourish's theory of the perceptual history of human-computer interaction helps explain information security through perceptions and interactions.

Dourish identifies four phases of human interaction with computers. The first was the electrical one. The computer was an analog machine made of single-purpose electronic components. Its programs were not digital but physical artifacts created externally and entered within the computer's memory via hardware (Dourish 2001, 5-6). The second phase was symbolic. Humans interacted with computers via alphanumeric codes that abstracted the numerical machine language of computers (Dourish 2001, 7). The third phase was textual. Humans interacted with computers using teletype and video terminals (Dourish 2001, 9).

The next phase, set in the 1980s, was graphical. Graphical interfaces with icons supplemented symbolic and textual interactions allowing users to manage information through screen space (Dourish 2001, 11).[3] For Dourish, tangible and social computing is the next phase of human interaction. I prefer to label them as networked appliances and multimodal ubiquitous computing. This allows the inclusion of mobile phones, drones, cars, and computers that react to different sensory inputs such as sounds, touch, and gestures (Dubé and McEwen 2015).

[3] Dourish does not explain where he classifies the computer mouse and related peripherals in his taxonomy. I place the mouse directly between the textual and the graphical phase as an artifact that enabled and facilitated the negotiation of virtual space through physical space.

Dourish's perceptual theory of interaction explains embodied interactions but not preconceived perceptions that influence both users and the operators that create the technologies. One way to approach perceptions is to use Don Norman's (2013, 41) adaptation of mental and conceptual models for HCI[4]. A conceptual model is the explanation of how something works (Norman 2013, 27). Mental models are the idiosyncratic conceptual models users devise to explain their interactions with technologies based on their perceptions of how things work (Norman 2013, 25-27).

It appears that Norman frames his theory of mental models from the experimental psychology branch known as psychophysics (Mackenzie 2013, 44). Psychophysics is based on the statistical measurement of information in the form of stimuli that people gather from their environment (Gepshtein 2010). People can confer meaning to processed information according to pre-existing mental constructs (Mackenzie 2013) developed from their memories (otherwise known as mental models). The definition of mental models chosen by Norman adheres to cognitive science perspectives. According to cognitive psychologist Philip Johnson-Laird (2010), mental models are shortcuts humans create from the perceptions they have derived from the world to lessen their cognitive load and reliance on reasoning to solve everyday problems.

But perceptions are not enough to construct mental models. A person must be aware of information received and meaning attached to it before any action resulting from the perception occurs (Dretske 2006). One method used by HCI researchers to understand a person's mental model is asking him to document it in a self-made drawing (Otter and Johnson 2000). As Norman argues, mental models are metaphors (Norman 2013). Metaphors are images and representations of objects by a subject.

Conceptual and mental models for similar objects can and do differ (Norman 2013, 27). How engineers and users perceive their interactions with information systems involves ever-changing conceptual models. Norman (1986) labels conceptual models created by designers, architects, engineers and developers (instigators) as design models. By adding design models as

[4] Norman's work on mental models adapts Johnson-Laird's theories to HCI (Johnson-Laird 1983)

a class of conceptual models created by technology creators, I acknowledge codified and documented conceptual models that originally shape the design of a technology.

The design model is not a blueprint that determines the course of the interaction between a user and a technology. The design model is about how things work from the perspective of the instigator of a technology. The social shaping of a technology (Feenberg 1999; Lievrouw 2002; Pinch and Bijker 1987; Williams and Edge 1996) by users' mental models allows them some agency over their perceptions about their interactions. The design model is not the technology. Rather it is the documentation about how this technology operates. By only creating the mental model, Norman created an asymmetry about the types of conceptual models held by users and architects. The counterpart to a user's mental model was a conceptual model. I am rectifying this by adding the design model as a new class of conceptual model. While design models are defined as not being user-designed (Gentner and Grudin 1996) they have not been differentiated the way I do in this study.

Design models interfere with user interactions with information systems. Design models are the conceptual models of how a technology works as conceived by its authors. A design model can potentially deprive users of control and participation in the elaboration of security and confidentiality enhancing practices by invalidating all or parts of their mental models. Designing information systems that enable confidentiality and security protection is a concern that has motivated different parties to find suitable solutions to protect end users. However, for measures to be effective, they must be user-centric. Users cannot rely on information systems, secure or unsecured, that are rendered unusable because they conflict with their mental models.

When a series of design models become a norm adopted by many technology instigators, they become a standard. Standards can be either documented or conceptual. Science and technology historian Jeffrey R. Yost argues that the need for standards influenced the first computer security designs (Yost 2007). Standards, he writes, were promoted by the American government, and specifically established by its military to create system interoperability between combat equipment and to conveniently provide access to resources such as larger computer facilities (Yost 2007).

2.3 History of Security through Interaction

Security was not the main objective for the development of standards by the American military. What was sought was structural and organizational usability. Yost argues that the security that standards brought was to provide safety for the physical resources and environment around computers to protect the integrity of their data and to provide public safety measures (Yost 2007, 597). For example, the TEMPEST[5] standard dealt with limiting the electromechanical radiation of computers (Yost 2007, 599).

Computer scientists and security experts at the time worried about deciphering data based on the electromagnetic emanations released by computers (Yost 2007, 599). Information security, Yost writes, existed because few operators had access to the large computers of the mid-20th century (Yost 2007, 600). Just like the Chinese of the 18th century who, according to intelligence historian David Kahn, failed to develop proper cryptographic measures because so few Chinese could read (Kahn 1996, 74), information security in the early computers was enforced through obscurity.

Obscurity measures could no longer satisfy security needs in the 1960s and 1970s because of shared-computing. Shared computing allowed teams of multiple users to use the resources of one computer such as the same database or library for an application used by several users of the same computer (Saltzer and Schroeder 1975). For example, Yost argues that shared computing which increased the level of user interaction and security risks in the military led to the creation of classification schemes such as top secret, secret, confidential and unclassified (Yost 2007, 604). New design models crafted by security experts controlled the human-computer interactions of military personal. Here, the classification of the documented information defined the level of interaction and access.

[5] TEMPEST is the acronym for an electromagnetic standard used by the United States of America to control for the capture of data emanating from hardware and software. Tempest (SANS Institute Reading Room 2017; Kuhn and Anderson 1998). MI5 intelligence officer Peter Wright first captured emanation from electromagnetic signal accidentally when trying to decipher French diplomatic communications between France's UK embassy and Paris in the 1960s (Wright 1987, 110-112)

Authentication grew from this shared-computing environment and spread non-uniformly to personal computing and now networked computing. While external security risks continued to exist in the age of personal-computing, errors[6] occurring during user interactions were important information security risks. Usability and personal-computing literacy played a role in what kind of errors users made. While multiple users could still use the same personal computer, the risk was less about centrally located data and levels of access by various parties.

Another dimension brought on by personal computing, according to Yost, was the privacy and the personal space between the user and a computer. Privacy concerns related to computer usage became a public issue in the late 1960s (Yost 2007, 616). He argues that large databases containing confidential information could erode the privacy of the people at a time that networking and information sharing through the Internet and related networked technologies were not prevalent (Yost 2007, 616). Here, the confidentiality of the information that is at stake was not that of users generating data through their direct interactions with computers. It was the information collected about people. I argue that it was not privacy that was at risk. It was confidentiality.

2.4 Usable Security and Privacy

Confidentiality, privacy, authentication, and security are topics frequently researched by usable security scholars. However, each issue tends to be addressed separately or in pairs only. For example, issues such as authentication and security are sites of study but seldom are authentication and privacy combined in one research as I am doing in this dissertation.

Scholarship in usable security attempts to merge the knowledge and practices of scholars and industry from information security with that of their human-computer interaction colleagues. It appears easier for HCI scholars to argue that the utility of usable security is in understanding

[6] To understand errors, it is important to remember Norman (1983, a)'s taxonomy of deviation from an intended action or a flaw in the formulation of an intention by a person. In the context of personal-computing, such errors can be a mistake in identifying threats such as phishing attempts, or misidentifying the purpose of an icon in the user interface of a program. They can also be errors in performing tasks such as slips when attempting to recall a complicated password, or failing to retrieve a backup of a document.

how people interact with information systems and other technologies. Whether this involves security or privacy is of interest to researchers concerned with human interactions. The utility of usable security may appear self-evident for security experts but may not be enacted in practice or in research. Of course, people matter in security, and of course how they interact, through engagement or circumvention with security systems should be analyzed by scholars, as security experts might say. But much of the jargon and the knowledge of how to research people is knowledge and practice that is known and customary with HCI scholars. What information security scholars contribute are a deep knowledge of the security standards, their flaws, and their utility in technological ecosystems.

Much of the early literature from the emerging discipline of usable security was focused on proving the limits of information security practices on users. As mentioned above, Adams and Sasse's "Users Are Not the Enemy" (1999) researched how users created schemes to bypass security measures in enterprise authentication systems. Whitten and Tygar's "Why Johnny Can't Encrypt" (2005) became a model for a series of research showing the usability limits of security schemes meant to protect users.

This focus on demonstrating the limits of existing security schemes with users has led much of the usable research to focus on authentication, an important site of interaction between users interacting with technologies meant to secure them and their data. Such research can focus on comparative evaluation of major authentication schemes (Bonneau, et al. 2012) or focus on specific schemes such as biometrics (Coventry 2005), graphical passwords (Monrose and Reiter 2005), or even captchas (Yan and El Ahmad 2008).

While other areas of interest to usable security researchers include email, messaging, and encryption, the most distinct area of research in the discipline is privacy-related. Privacy-related usable security research has become important enough to feature equally as an area of concern to security in specialized venues such as the *Symposium on Usable Privacy and Security* (SOUPS). Privacy research pushes usable security away from its purely instrumental origins and begins to address societal concerns related to how people interact with technology in the information economy.

Privacy can be a difficult concept to explain in everyday human-computer interaction. Management scholar Mary Culnan (2000) defines privacy as the control individuals have over their personal information. Using Culnan's definition as their starting point, scholars Mark Ackerman and Scott Mainwaring (2005, 382-383) describe privacy as being individually subjective and socially situated. Individuals perceive privacy differently based on the application and the context of usage. For example, they argue that users perceive privacy differently when using personal banking and social media (Ackerman and Mainwaring 2005, 383). Users may perceive their information as private when using a personal banking system. On a social media Web site, users may feel freer to share their information publicly. Usability scholar Benjamin Brunk describes scholar Eli Noam's definition of privacy as "the place where the information rights of different parties collide" (Brunk 2005, 402).

These different privacy definitions echo the social theory debate of agency (the individual) versus structure (the system) described by sociologist Anthony Giddens (1984).[7] For Culnan (2000), Ackerman, and Mainwaring (2005), individuals have primary control over their privacy. For Noam (1997), privacy is a collective trust many parties control. Agency versus structure also characterizes the privacy practices, perceptions and interactions with technology systems. While individuals attempt to adjust what information is disclosed about them (Cranor 2005, 448); cryptologists see privacy as technical systems; the European Union has moral expectations that American policymakers lack; sociologists perceive social nuances ignored by engineers (Lederer, et al. 2005, 422).

Privacy, however, is not the only protective concern of information architects at the design stage. Several scholars perceive privacy as a component of security (Mihajlov, Josimovski and Jerman-Blazič 2011; Bonneau, et al. 2012). While developing a framework to evaluate usable security in authentication mechanisms, scholars Mihajlov et al. (2011, 333) have

[7] Giddens (1984) identified a debate where sociologists following World War II argued that the primary actor for social action was based at the level of societies, and that individuals' actions were influenced by these structures (societies). But this ontological debate about the nature of social action was challenged by ontological interpretive approaches such as phenomenology where the individual (the agent) was the prime agent of change (Giddens 1984). Giddens theorized with structuration theory that both structures and agents were dualities of one another.

included privacy as one of many criteria. In a similar study evaluating the usability, deployability, and security benefits of alternative authentication methods, Bonneau et al. (2012, 5) describe privacy as a component of security. This appears contradictory to the usual framing of security as constraining privacy, especially in a post-9/11 world plagued by surveillance and information controls (Bambauer 2013; Deibert 2012). The nature of security that I investigate is pertinent to individuals as opposed to states and organizations. It is about the personal security of individuals that includes their privacy as they interact with information systems. However, in practice, when information systems retain personal information about individuals, they do so in confidence and under the tacit or explicit agreement of users (Siegel 1979). Therefore, it is more appropriate to say that it is confidentiality that is protected rather than privacy.

In the next chapter, I propose the transactional token, a theoretical framework which builds on the literature covered in this chapter to explain the commodification of users' data as they perform tertiary authentication. Literature related to HCI, risk, information security and usable security seldom attempts to explain what role and motivations platform operators bring as they offer people authentication mechanism. The transactional token framework draws from commodity theories and related Marxist literature to explain the process of commodification that results from user interactions with platforms through authentication. I start the Theoretical Framework chapter by defining the forms of authentication used in this research. I end the Theoretical Framework chapter by introducing conjectures that will be elaborated in the Research Approach chapter (Chapter 4) and tested in a Quasi-Experiment (Chapter 5) and a Policy Analysis (Chapter 6).

Chapter 3
Theoretical Framework

In this chapter, I define the three forms of authentication that I have introduced in the introduction chapter. I differentiate primary, secondary, and tertiary authentications so that these definitions can be reused in the transactional token theoretical framework developed for this study. This framework is used in later chapters such as the policy analysis, and the discussion to explain how tertiary authentication can lead to the commodification of people's personal information.

I provide a brief review of works related to the commodification of audiences in the information economy. I start by analyzing the work of Karl Marx who contributed much of the early work on the theory of commodification. By drawing on Georg Simmel and Erving Goffman's work I can theorize interaction at the individual level while providing a critical perspective based on commodification theory.

Marx presented a macro-analysis of societal structures which differs from the human agency focus of Simmel and Goffman. Because this study lies at the crossroads of HCI and critical information studies, I rely on both macro and micro theorization and evaluations.

My transactional token theoretical framework is based on a dialectical approach which I explain before discussing each step of this model that I have chosen to represent as a diagram. The diagrammatic nature of the transactional token framework reflects my personal research and professional background in visual literacy and visual research methods. Because the diagrammatic nature of the transactional token is at the heart of my arguments, I present parts of this model visually throughout my discussion of the components of this theory of audience commodification.

I end this chapter with a presentation of the three conjectures I tested in the study's design using a policy analysis and a quasi-experiment. The use of the three conjectures is an operationalization of the research questions presented in the first chapter to test some of the study's claim empirically.

3.1 Forms of Authentication

Using Dourish's embodied interaction theory of human-computer interaction (2001) I make observations about users' and developers' conceptual models of information security interactions. As mentioned in the literature review, Dourish theorizes four phases of human interaction with computers. They are the electrical phase, the symbolic phase, the textual phase, tangible and social computing. In his work Dourish seeks to shift the perception of computers as physical machines with which people interact with to a perspective that focuses on the social context of computing (2001, 5).

The advent of personal computers along with portable media like diskettes enlarged the user base while creating new information security risks. Although information security risks related to space and interaction persisted, maintaining the confidentiality of recorded information emerged as a novel challenge for security experts. Finally, with ubiquitous computing and general networking, space returned as a risk for information security. Information readily travels from one computer to another through networks. The site of interaction between a user and computer, which I define as the place physical or abstract where the user person interacts with the technology, is now part of a wider network of exchanges threatening the security of people and information systems.

The forms of authentication that I define below are not analogous to authentication schemes such as the password, paper token, hardware token, phone-based, biometric, graphical, federated, etc. (Bonneau, et al. 2012). Instead of focusing on the physical device, I emphasize the interaction between the user and the information system. Thus, I define these forms of authentication as primary, secondary, and tertiary. While most primary, secondary and tertiary authentications are password-based, they can rely on other schemes or a combination of schemes, like phone-based, graphical, biometric, and federated alternatives.

From the cross-pollination and interplay amongst various information systems and third-party services, a taxonomy of modes of authentications based on the accessed domain can be developed. The first type of authentication is primary authentication. With primary

authentication, once her identity has been verified, the user accesses the resources of the platform where she has logged into.

With secondary authentication, the verified user has access to other information systems owned by the same platform operator. The services can be different or complementary. Yet, the user, theoretically, could log into the secondary information system, without having performed an authentication in the primary system. Some of the user's information is transferred from the primary system to another. Some operators with many services use a common authentication for multiple services. For example, Google offers users access to several services like Picasa, YouTube and Analytics through a secondary authentication.

With tertiary authentication, the user provides her identity for verification before using the resources of a third party. It provides the third party access to the user's resources on the primary system. Tertiary authentication relies on the user to perform the verification of the third party's identity before the primary system grants access.

The literature on information security currently does not differentiate similarly between the types of authentication I have classified. Authentication mechanisms that rely on tertiary methods have been discussed, such as single login (Payne and Edwards 2008; Waters 2012). The focus of the authentication literature is instrumental. It focuses on the operations used by a single authentication method instead of conceptualizing authentication from the point of view of the user and his information. My taxonomy of authentication pays attention to the interaction of the user with an information system. It recognizes when a user interaction requires more steps and the involvement of secondary and tertiary parties without dismissing traditional instrumental taxonomy information security experts use to describe various authentication methods.

I have identified three kinds of tertiary authentication systems. The first kinds are tertiary apps that mimic the primary platform they rely upon in their authentications. For example, Twitter client apps like Talon replicate the primary service. They offer a modified user experience distinct from the primary system. The second kinds are the plug-in systems that add features or manipulate data from the primary one. Hootsuite has this particularity. It adds moderation and curation to help users track various social media. Finally, some systems offer

new services and products. Still, they pull user authentications from existing platforms. For example, Medium offers a blogging platform with separate services and features. Yet, it relies on Twitter and Facebook to authenticate its users. **Table 1** includes a list of the three forms of authentication, the three types of tertiary authentication referred to below, as well as examples for each form.

Table 1 - Forms of Authentication

	1ST EXAMPLE	2ND EXAMPLE	3RD EXAMPLE
PRIMARY AUTHENTICATION	Facebook	Google	Twitter
SECONDARY AUTHENTICATION	Instagram	Google Docs	Vine
TERTIARY CLIENT APP CLONE	Playbook Facebook Clone	Spark	Talon
TERTIARY DATA MANIPULATION APP	dlvr.it	Business Organizer for Google Docs	Hootsuite
TERTIARY SERVICE & PRODUCT APP	AngryBirds Friends	Dropbox	Medium

Tertiary authentications may contribute to the erasure of personal and professional borders within the lives of users. As sociologist Erving Goffman (1971) might argue, users' practices and self-representations change based on the context permeating their lives. People may use one device for both personal and professional work to generate personal data and interact with others. Thus, what apps they use, may influence how they present themselves when interacting with information systems. Social scientist Hugh Miller (1995) had a similar idea when he extended Goffman's interaction theory to online browsing and electronic life to argue that how people presented themselves in personal websites was different than face to face presentations.

Although not a matter for evaluation, in this study I argue that different primary platforms lead to different types of interactions and user practices. Some primary information systems that support tertiary authentications appear to support professional activities. SharePoint,

LinkedIn and Dropbox are work and professional platforms that individuals can use in their everyday lives. They support authentication by groups engaged in collaborative work.

Other platforms such as Google+, Twitter, and Facebook rely on the individual as the first level of authentication while enabling additional groupings to be added to the original individual level. I readily admit that these distinctions are more fluid than presented here with the evolving architectures of these platforms. For example, Google offers a suite of collaborative tools for organizations, such as the management of institutional emails through its Gmail platform. Likewise, Dropbox, while meant as a collaborative tool to exchange data with others, also requires its users to create individual accounts first. These accounts, of course, can be used for nothing but personal back up utilities. To manage the scope of this study, I have decided to focus on the three primary platforms whose basic unit level of authentication is the individual user (Facebook, Google, and Twitter) and to exclude an evaluation of collaborative platforms such as Dropbox and LinkedIn.

3.2 The Transactional Token

My theorization of the transactional token explains the process where data is exchanged from one information system to another as a commodity. Explaining this process sheds some understanding about how the commercialization of users' data affects their security and confidentiality. It explains what really happens with users' data and why they should care about their security and confidentiality.

The transactional token model introduced in this chapter has two branches. One branch explores authentication, the other, the commodification of user data. Looking at the first branch, I perform a macro-level analysis of authentication. When exploring the second branch, I perform a micro-level analysis of the commodification of user data using interaction.

In the context of this study which bridges human-computer interaction with critical approaches in communication and information studies, an analysis using a combined macro and micro-level analysis is relevant and essential. Because human-computer interaction studies often rely on empirical methods such as experiments where an evaluation of a sample of participants is

generalized to a population at large, it appears as a discipline focused on discreet interaction performed by individuals.

3.2.1 Related Work

In this section, I review works by several scholars on the nature of the commodification of audiences and how it relates to authentication. The commodification of audiences is an expansion of Marx's (1990) theory of commodification applied to viewers of radio and television contents by Canadian scholar Dallas Smythe (1977). Smythe's theory of audience commodification has been extended by critical scholars such as Christian Fuchs (2012, a; 2012, b; 2014), and Mark Andrejevic (2017; 2013; 2014). But this theory departs from Marx's original argument in that instead of people's labour becoming commodified, it is people as viewers who become commodified. Thus, I also review some of the arguments by communications scholar Brett Caraway (2011) that seek to adjust the theories of audience commodification, especially in the context of the information economy. Critical scholar Tiziana Terranova's (2004) take on the commodification of audiences is to explain why people feel compelled to participate in the information economy, which supports the further commodification of their labour. I contrast Terranova's take with that of jurist Johnathan Zittrain (2008) whose liberal perspective explains the necessity and inherent opportunities of information systems that allow users' personal information to move. In Zittrain's view, personal information is not a commodity but a variable that forces change (2008). Before looking at these authors, I explore Marx's theory of commodification in depth and contrast his structural theory with that of Simmel (1978) and Goffman's (1971) work on interaction.

Tertiary authentication transforms the user's personal information into a commodity exchanged between information systems. This personal information, like money is exchanged as a good between parties. Marx (1990, 2) defines a commodity as a good whose properties satisfy human needs and is produced for the purposes of exchange.

People are not commodities. However, according to Marx (1978) people can sell their ability and willingness to work as a commodity. Marx referred to this commodity as labour power (1978). The transactional token discussed here is much like Marx's labour power. The

transactional token is a commodity drawn from people but not a person. Instead, users' interactions with technologies involve processes that can be commodified. The data exchanged between two systems about a user can be exchanged as a commodity. The capacity of tertiary authentication to verify the identity of a user accessing an information system constitutes its use-value. Its capacity to be bought and sold constitutes its exchange value.

Marx expands his inquiry of the exchange value by investigating money. Money is a commodity that allows value to be stored as a universal equivalent to facilitate exchange between commodities by replacing it with an object (Marx 1990). Money takes forms such as coins, token, paper currency, or credit (Marx 1889; Harvey 1989).

Simmel has a different perspective on money. His perspective, unlike Marx, focuses on the utility of money in interactions. Unlike Marx, he does not approach money as a structural concept that shapes societies. Simmel cares much more about money and its relationship with the individual. He describes money as the agent that creates distance and further abstractions between subjects and objects (Simmel 1978, 62). Value, he argues, is created through the act of overcoming the distance between the subject and its object of desire (Simmel 1978, 63-64). Simmel further argues that exchanges are the most developed form of interaction humans use to acquire products and information (1978, 79).

Simmel describes interaction as a macro-level practice while exchange is a micro-level one (1978, 80). With interaction, the subject offers what she does not have. In an exchange, the subject offers what he possesses (Simmel 1978, 79-80). While interactions often take the form of exchanges, they do not necessarily involve the addition of gains or the loss of value that characterizes exchanges (Simmel 1978, 79-80).

Simmel posits that money regulates all exchange values in modern life by transforming emotional relationships, a form of interaction, into quantitative abstractions (2002, 12). With money as a means of exchange, the customer loses the direct interaction with the producer while struggling to maintain a distance between personal life and social life (Simmel 2002, 12).

Marx and Simmel represent two classic views of the structuration debate that pits societal structures against human agency. Both Marx and Simmel represent the dynamic which I attempt

to resolve with the framework. This tension is important in the context of this study which attempts to combine HCI and critical information studies traditions in one research project.

The struggle to overcome personal and social distance, as described by Simmel, is another way to perceive the conflicting and changing self-identities described by Goffman (1971), earlier. While Simmel described interaction as a burgeoning conflict in the *fin de siècle*, it is an emerging area of resistance and transformation in the information economy. Tertiary authentication is an example of the transformation of interactions into value exchanges moderated by money.

Simmel's understanding of money and its effect on people differs from Marx who focuses on the structural changes that money, as a commodity has on societies. Instead of being an abstraction that creates distance between people and their wants, money determines the value of various objects. Borrowing from Marx, geographer David Harvey (1989) describes a similar phenomenon. Money, he argues, has become a fetish for social labour. Social labour, he argues, is the source for the production of commodities (Harvey 1989).

Communication scholar Dallas Smythe (1977) changed the perception of social labour and commodities arguing that in the period of mass media, leisure time is productive labour time where consumers perform unpaid labour by consuming advertising and learning to buy the goods and services marketed to them. Here Smythe argued that instead of just alienating workers from the means of production through a monopolistic capitalist economy, mass media functioned to indoctrinate workers into consumerist mindsets (1977). Workers have access to cheap mass media whose content is paid for by advertising encouraging them to purchase more commodities (Smythe 1977). Thus, the reduction in total work time achieved through class struggle and organized labour was not a reduction but a reallocation of production time into the personal lives of workers (Smythe 1977). This reallocation of productive space into personal space parallels the blurring of professional and personal lives that Goffman described.

Caraway (2011) characterizes Smythe's audience commodity as a simplification of Marxism banalizing the agency of consumers and workers in the commodification process. According to him, Smythe's theory treats audiences as agreeable participants in the

commodification process without any resistance (Caraway 2011). Smythe, he argues, attempts to generalize productive labour as an ongoing practice that audiences cannot escape (Caraway 2011). By doing this, Smythe conflates his audience commodity with working class subjectivity (Caraway 2011). Doing so he argues that people are commodities, thereby foreclosing any substantive analysis of working class struggle against the processes of commodification (Caraway 2011).

Contrarily, communication scholar Christian Fuchs (2012, a) argues that audience commodity theory, as argued by Smythe is directly applicable to social media. He maintains that social networks like Facebook, Twitter and YouTube commodify users' data that they resell to advertisers through various means (Fuchs 2012, a). Social networks, he claims, make full use of audience's leisure time, offering access to contents and a communication channel in exchange for data and behavioural metadata (Fuchs 2012, a). Fuchs characterizes capital not as money but as accumulated money (Fuchs 2012, a). For Fuchs, even individualized creative production created by platform users is a form of commodification of their labour (2012, a).

Basing his analysis on Smythe's commodification of audiences' theory in a 2012 article, Fuchs evaluated Facebook's privacy practices and argued that the social network was attempting to commodify users and their data (Fuchs 2012, b). Fuchs's approach differs from the one I demonstrate in the transactional token framework presented below. I explain every step leading to the commodification of personal data by analyzing the process at every site of interaction between user and machine.

For communication scholar Marc Andrejevic, the collection of data from users' information practices feeds the predictive surveillance technologies of states and large Internet companies such as Google who monetize the information of users, which they treat as their own property and even refuse, in some instances to return (2007; 2013). While Andrejevic does not deny that users have some agency in the data produced about them, this product activity is a separate entity from the worker that helped its generation. In a sense, the harvesting of the information is a practice performed by states and Internet companies as opposed to a good produced by users. This information was extracted from users but it is not part of users. My approach to user-generated labour focuses less on what they create but more on the performance

of authentication with one's identity. User-agency is inherent in authentication. It is a form of interaction where users share an abstraction based on their selves in a verification process in exchange for access to an information system. As I argue later in this chapter, the user is not his identity. Identity is a space created by the user through interaction with an information system that can be exploited and commodified by third-parties. I cover the relationship between the user and his identity below.

How third parties use the information collected from people's information practices is not always negative. Zittrain argues that open systems allowing third parties to deploy services that can add, delete or modify data foster innovation and disruption that benefit platforms (2008). Zittrain argues that open systems as generative technologies undergo transformations that ultimately benefits users (2008). He also argues that traditionally, greater allowance for flexibility and interoperability increased security risks (Zittrain 2008, 9). Tertiary authentication appears to be a hybrid of both open and closed systems that vary from platform to platform. Facebook, Google, and Twitter are proprietary platforms. Yet, users' personal data can still flow from them to third-parties easily through tertiary authentication.

Platforms that enable the sharing of primary authentication between primary and third parties attempt to add security to protect their users. Popular platforms straddle a fine line between being open and closed systems. When platforms are closed systems relying on proprietary technology and captive user data, they do not foster transformation by keeping their users locked. A lack of incentive to transform a platform can stifle its growth and development and market competitiveness. Closed platform's architecture reinforces and benefits from control over transactional tokens.

Scholars such as Smythe who argue that people's labour is the basis of the commodification of their information do not frame their observations using the closed versus open platform perspective. The premise of the audience commodity theory is that viewers perform labour by consuming advertising and learning to become consumers of advertised goods and services while consuming entertainment and information provided by contents providers and platforms who sell people's attention to advertisers (Smythe 1977). Audiences, which for

Smythe also included readership, in the form of printed media, were sold as commodities by media operators to advertisers.

Audience Commodity theory has been controversial but accepted by many critical scholars of communication (Meehan 1993). With its origin in broadcasting and the measurement of television audience, audience commodification has found relevancy in research related to advertising and the measurement of attention in the information economy.

Information as a commodity was what first interested critical scholars from a generation ago. For example, communications scholar Benjamin Bates (1988) explored information as a commodity, attempting to determine its value. Shoshana Zuboff (1984) explored the process of documentation and automation of workers' labour practices. Philip Napoli (2014), following Eileen Meehan's (1993) lead from a generation ago argues that user metrics and ratings is the core value of audience commodities. His research explores the traditional television setting but focuses on how social media can better capture audience metrics (Napoli 2014).

However, other critical scholars trained in the audience commodity tradition analyze user's information practices as it relates to digital media. Jason Pridmore and Daniel Trottier's (2014) research focuses directly on social media's role in the generation of audiences. Detlev Zwick and Alan Bradshaw (2014) explore the mining of virtual online communities for commodification. Micky Lee (2014) focuses on audience commodification regarding search engines, particularly Google, and the monetization from Google AdWords (2011). Mark Andrejevic (2014) studies the expansion of audience commodification from audience selling to the reselling of audiences' meta-data and behavioural data in online venues. Vincent Manzerolle (2014) investigates the audience commodification in mobile and ubiquitous devices. Scott Kushner (2016) discusses the implication of lurking behaviour online and how platform operators must adapt their audience commodification metrics to continue user profiling. Kenneth Werbin (2012) draws a link between people's personal information available online to audience commodification. Fernando Bermejo (2009) writes a history of tracking metrics used for broadcast television all the way to online metrics used today.

One of the criticisms against audience commodity theory has been the lack of measurement and study of the people being commodified (Caraway 2011). The process of commodification of audiences is not something explored often. For example, Zwick and Bradshaw (2014) mention several strategies but do not analyze the exact means used to achieve the commodification. Measurement of audiences, as explained by Meehan (1993) can be tricky. But while measurement captures data about audiences, it does not tell us much about their interactions. For example, one could put a Nielsen television tracker on a dog to trick the device into thinking that people were watching television.

Information systems reveal much more information about audiences than television because people leave metadata about themselves when they interact with technology. While online advertising through Google Ads and search engines can reveal a lot about people's information practices (Lee 2011), authenticated users can feed and provide more data which can lead to the commodification of their attention.

Scholar Frank Pasquale (2015) defines four types of user tracked data. They are the self-tracked; data tracked from an interaction with an information system; third party tracking performed by an organization verifying records left behind by users; and fourth party data, which is data brokered by parties that purchase and resell user data (Pasquale 2015). Many of these types of data feature in the transactional token model but are presented through different taxonomies. Self-tracking data, for example, is something people performed when authenticated. However, in the transactional token model this can occur anywhere, once the user is logged in.

An alternative theory to audience commodity has been the attention economy theory introduced by economists Herbert Simon (1971) and redefined by scholars Thomas Davenport and J.C. Beck (2002). This theory is based on theorization of human attention as a scarce commodity operating in the context of information overload within an information-rich world (Simon, et al. 1971). As more information is produced, the amount of attention required to consume such information becomes a scarce resource. An expansion of the theory of attention by economist Michael Goldhaber (1997) uses the Internet as the site where the information overloads occurs. Media scholar Claudio Celis Buenos (2017) has attempted a critical take of theory of the attention economy. He argues that attention – watching, reading, is labour (Celis

Bueno 2017). Attention is thus not a scarce commodity that platform operators fight over. It is work by audiences. Celis Buenos's theory runs parallel to audience commodity theory while maintaining stronger links to autonomous Marxism traditions. Keeping a critical stance on the attention economy, unlike Smythe, Celis Buenos does not claim that audiences are commodities. It is their labour which can be commodified. While not an aspect that I pursue specifically in my transactional token framework, Celis Buenos's approach is closer to my own position on the commodification of audiences.

3.2.2 Approach

The transactional token framework that I introduce is based on dialectics. Plato popularized dialectics in philosophy. For Plato, dialectics were a way to contrast the positions of Socrates, his teacher, against that of others arguing with him (Maybee 2016). Dialectics were interactive discussions where Socrates challenged the ideas proposed by an audience member with another (Maybee 2016). The process was based on contradictions in ideas (Maybee 2016).

Nineteenth century German philosopher Georg Wilhelm Friedrich Hegel took inspiration from Plato's *mis-en-scène* but changed the actors in his dialectics from people personifying positions to ideas being refined and redefined in a constant process (Maybee 2016). Earlier less elaborate ideas, defined by an unstable process challenging the fixity of the former (Maybee 2016). This challenge is a dialectical moment whose contrarian nature is only resolved through a third speculative process (Maybee 2016). The resulting stable definition is once again challenged (Maybee 2016).

Karl Marx was inspired by Hegel's dialectic model. However, instead of basing his interpretation of dialectics as a process of contradicting personae, like Plato, or ideas, like Hegel, Marx (1978) based his contradictions on the material processes that affected humans and their societies. In *The German Ideology*, Marx argued that Hegel and his followers (the Young Hegelians) based their philosophical frameworks, such as their dialectics, on arbitrary ideas disconnected from the material conditions of people (1978).

Marx argued that humans exist and that their social organization was the basis upon which notions about their societies and lives came from (1978). Philosophical ideas sprang from

the dominant ideologies espoused by the elites who controlled means of productions (Marx 1978). Thus, philosophy reflected dominant ideologies. Marx challenged this system by arguing that the means of production and reproduction of humans should be used as the core dialectical units in philosophy (1990). This perspective is known as material dialectics.

The transactional token framework introduced here does not adhere to strict thesis-anti-thesis-synthesis forms where an initial concept is split in two opposing notions and reunited thereafter. The transactional token framework I present veers and splits in different paths as needed. Hegelian and Marxian dialectical philosopher Christopher J. Arthur (2002, 8) explains that the main purpose of dialectic as used by both Hegel and Marx is to extend ideas into logical categories (Arthur 2002). Dialectics are a taxonomy of philosophical thoughts and social theory.

Marx's dialectic framework for capital is essentially non-historical (Arthur 2002). While Marx's explanation of the modes of capitalism were historical, that is the tribe was followed by serfdom, which was followed by mercantilism, which was followed by industrial capitalism and so on, his commodity framework was not. As Arthur explains, any point in the chain could be the starting point for the inquiry about the nature of capital (2002).

The transactional token, much like the commodity dialectic framework that inspired it is not historically-based. However, the framework I introduce below is based on authentication as the start of the process of commodification of users' data. There is a material quality to this model based on interaction of a user with an information system. Without that act, the process of commodification changes although as will be seen, it continues under a different form of commodification that is not the transactional token.

But once the user has logged into the platform the non-specificity of an ahistorical process that characterizes Hegelian and Marxian logical dialectics follows through with the transactional token. Some branches of human-computer interaction often portray the interaction between a user and an information system as a linear process. For example, Fitts's Law calculates the movement time a human limb such as a hand move towards a designated target, such as mouse (Card, Moran and Newell 1990, 51). The Power Law of Practice accounts for the variability of performance of a person performing a repetitive task such as using a keyboard

(Card, Moran and Newell 1990, 57). The range of interactions between the user and the information system are limited by options predesigned in the technology. This way of understanding HCI locks the possibilities in a black box (Pinch and Bijker 1987).

It is more the case, that human interactions with information systems are varied and indeterminate. Every interaction is discreet. Human error and reaction from both humans and technology to events such as errors can take many shapes. Humans have agency over how they react to technology.

This randomness and agency which causes a variety of discreet interactions is why a clear dialectic approach where the process of thesis, antithesis, and synthesis forces the predetermination of actions when a person performs an authentication task. My transactional token model starts at the first site of interaction and then allows for a multiplicity of experiences and interactions between humans and information systems.

Interaction between people and technology can be seen through the lens of interaction between subject and object. While Lucy Suchman (2007) argued that such interactions were an assemblage, Simmel proposed that everything interacts with everything (Davis 1997, 380). Both subject and object attempt to influence one another into frames of references that organize the relationship between two independent agents (Davis 1997, 380), whether they are human or machine.

When the user performs an authentication with an information system the site of interaction between the subject and the object has random possibilities of outcomes based on the self-perpetuating agency of each agent and its effect upon the other. The transactional token exemplifies the greed described by Simmel when interactions between subjects and objects occur (Davis 1997, 380).

3.2.3 Discussion

As the demonstration of the transactional token framework progresses, I introduce several terms which may appear to refer to well-established phenomenon and concepts. When the definition of the terms differs greatly from the relevant received literature, this will be indicated.

3.2.3.1 The Commodity

The transactional token is the starting point of the framework. The analogous starting point in Marx's dialectic is the commodity. The commodity according to Marx, is something that satisfies human wants and is produced to be exchanged for something else (Marx 1990). It is also the primary unit of accumulated goods in capitalist economies (Marx 1990).

According to Marx, the nature of the commodity is qualitative and quantitative (Marx 1990). The qualitative aspect of a commodity is its use-value, or what it is good for (Marx 1990). The quantitative aspect of a commodity is its exchange value, or how its value is measured (Marx 1990). Marx argues that a proportion of use-values are exchanged against a certain exchange value (Marx 1990, 126). Use-value and exchange value are related aspects of a commodity.

Marx begins his dialectical framework with the commodity, splitting it into two antitheses and explains them as quantitative and qualitative forms of value. But within each antithesis, Harry Cleaver (1979) argues, there is an internal conflict where the use-value, for example, has both qualitative and quantitative properties. Similarly, the exchange value, which Marx describes as a quantitative value, internally presents qualitative properties (Cleaver 1979). It is only through the reunification of the exchange value with the use-value that their internal inconsistencies are resolved (Cleaver 1979). However, the resolution becomes a new synthesis, which is value.

One popular way to explain Marx's dialectic model has been Harvey's (2010) approach. Unlike Cleaver, Harvey does not graph the internal dialectic conflicts within the antitheses. Instead, he simplifies the internal process by focusing on value, the next step in the Marx's dialectic chain. The graphs of Marx's dialectic can differ as scholars emphasize different properties of each thesis, antithesis, and synthesis.

A central theme in Marx's dialectic theory is that regardless of its permutation through thesis, antithesis, or synthesis, the commodity exists as a process enabled through human labour. Labour, as the source of value, is a process constituted by three basic factors: 1) work; 2) raw

materials; and 3) instruments of production. The magnitude of value for a given commodity is determined by the labour time that is socially necessary for its production (Marx 1990).

Marx links the value of labour to the exchange value. The exchange value becomes the measurement of the value of labour. Marx writes that only labour used to produce goods that have both utility and can be exchanged, matters to produce a commodity (Marx 1990, 131-133). **Figure 1** depicts Marx's commodity in a diagrammatic format adapted from David Harvey's representation (2010, 26).

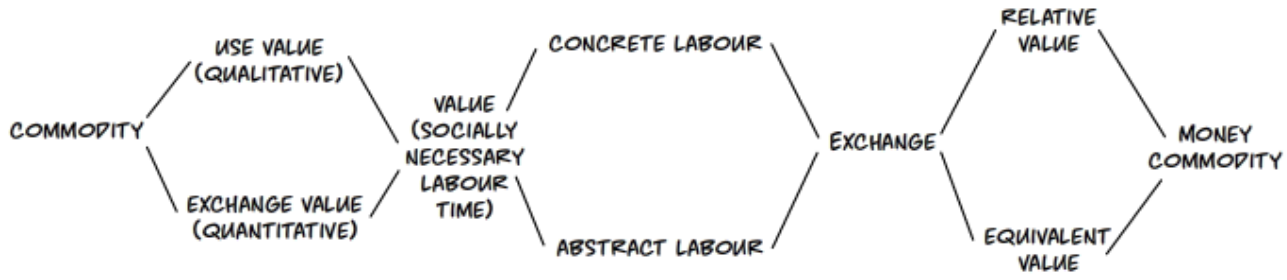

Figure 1 - Marx's Commodity (Harvey, A Companion to Marx's Capital 2010, 26)

3.2.3.2 The Transactional Token

My claim in this chapter is that the transactional token is a commodity. As I explained above, the transactional token is the commodification of people's data as they authenticate themselves through multiple information systems. As a commodity, the transactional token takes the transient form of data produced through the labour of users performing authentication tasks with information systems. This authentication task is a form of labour.

However, the transactional token as a process is internally conflicted with both qualitative and quantitative properties. It has a dual nature, allowing users to authenticate themselves within an information system and beginning the process of monetizing users' attention. The dual nature of the transactional token is to protect users' data, while making it commercially available to the platform operators that provide access to their members.

There is a dialectic purpose to the transactional token where it provides a use-value – user protection of data and an exchange value – the commercialization of said data. As a commodity,

the transactional data is produced from users whose information is held in confidence by platform operators.

Smythe's audience commodification theory to some extent has parallels to the transactional token but they are superficial. For users, the use-value of the transactional token is the protection of their data. But where is the use-value in Smythe's audience commodification theory for the consumer of mass media? Smythe can readily identify the exchange value of audience commodification but does not propose a use-value. He could have suggested that advertising provides information about commodities, their prices to audiences. He could have made the media contents transmitted itself be the use-value but it is not an important aspect of his arguments. Broadcasters and publishers sell their viewers to advertisers.

Smythe does not identify a dialectic conflict within the audience as a commodity that has both a use-value and an exchange value. The audience itself is the commodity. The mass media that it consumes is not the use-value. The audience, following Marx's dialectic would thus consume itself and be its own commodity (Postman 1986). Smythe's theory explains the exchange value aspects but ignores the use-value to audiences (which I argue is media content). Neither does he claims that people's attention is a use-value for marketers.

Thus, the internal logic of Smythe's audience theory, if evaluated through the lenses of Marxian dialectic, is flawed. This flaw favours determinist propositions reducing complex interactions that people have with technology into simplified Marxist-influenced theories disregarding the complexities of Marx's dialectic. Its purpose is to find a "villain" for the proletariat (Caraway 2011; Cleaver 1979).

Smythe's audience commodification theory eschews Marx's dialectic and seemingly, does not need it to become a useful evaluation framework. However, the transactional token is based on a dialectic framework and obtains validity through its internal use. This again, is because of the dialectic nature of the transactional token whose use-value is the protection of user data and its commercialization by platform operators as an exchange value.

Authentication and the monetization of attention are pre-existing properties found within the transactional token. As mentioned in chapter one, authentication is often the only protection

between a user and risks while using a networked-information system. But authentication is also about verifying the identity of a person as a means of offering protection.

The monetization of a person's attention is more beneficial if the platform operator knows the identity of the person. Authentication provides platform operators more information about the validity of the data that they hold about users who interact with their information systems. Unverified users can also be targeted but the process is less certain.

Authentication and the monetization of attention split dialectically into two branches that I will explain individually. At times, these branches intersect into one another. But in the end, the two branches, one exploring a philosophy of authentication, and the other a social theory of monetization will merge back, following the dialectic model of the transactional token.

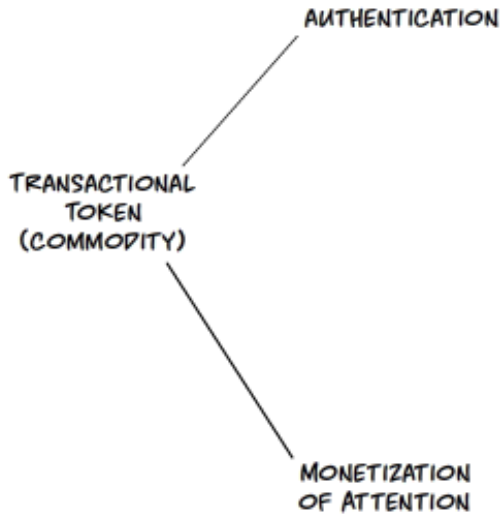

Figure 2 - Transactional Token - A Commodity

3.2.3.3 Authentication

Authentication and other security measures are impediments to users performing tasks (Adams and Sasse 1999). Users seek access to resources; however, they must allow the verification of their identities before access is granted. Access is what people want but they must trade in their identities to use an information system.

From the operator's perspective, authentication confirms the user's access to the platform. The time and place from which the user performs the authentication can be documented and quantified. The recording of users' authentication and usage by the platform operator is the first step into transforming data about people into a form that can be exchanged later as commodity with marketers.

The user interaction with an information system is quantified to allow access. The authentication is also a form of use-value for the user. Access to the platform is what the user seeks. Authentication provides this but also encourages the platform operator to protect and secure users' data. These are added use-values for users.

There is another form of use-value for the user. This use-value is found in the very authentication method used to access the platform and verify one's identity. A means of authentication, like a password, is a commodity kept by the user and only known to the operator who keeps it in confidence in a database. The user must preserve this means of authentication or it loses its value. A platform user can share or give away her password with another but doing so can reduce the use-value when account personalization and recommendations accrued through the exclusive preserve of the password, or token.

Similarly, the means of authentication, like a token or a biometric signature is a use value for the platform operator. It is a form of flood-control where the means of authentication is meant to be used by one user or a designated group. When the user shares this means of authentication with others, it devalues its utility as a tracking and documenting token. For example, when multiple users share one Netflix account, the customization of the users' likes and profiles is not as accurate. It represents the aggregate interaction of several people instead of one person.

Authentication appears to be a transient act. It appears to be something that happens only when people need to provide a verification of their identity when interacting with technology. It appears to be an extra act that comes between the subject and the object allowing the latter to recognize the former. Authentication appears to be an act that happens at a site of interaction and ends when a session with an information system ends. Throughout this framework, I will argue

that authentication is not an impediment that obstructs people's access to technology. Authentication occurs in people's everyday lives constantly, even when they are not using an information system. Authentication is omnipresent because people verify their identity to seek access to resources and spaces regularly. An authenticated session is nothing but an ephemeral session with an information system that does not account for the authentication that happens at other levels of abstractions and that allows the user to use one technology.

Philosophically, authentication is the reduction of ephemerality through the inscription of identity to a technology thereby creating a token used to verify the person (truth) and provide access to a realm (platform). Ephemerality, as I will explain in greater details below, means that it is a session where the user is authenticated but that does not account for all other forms of authentication that allow people to have access to technologies. Access to a technology and the verification of identity define authentication as a form of interaction. Though dialectically intertwined, we can analyze identity verification and technology access separately as two aspects of authentication that reveal more about how technology's ephemerality.

3.2.3.4 Identity verification

Identity verification can be understood as what is given and what is withheld. Identity verification assesses the credentials of a person to determine that her identity is true. Access is given to the person whose identity has been verified. But access can be withheld until the evidence of a person's identity has been verified. Hence, general opportunity to access a resource or a space is limited. The credentials used to verify people can take multiple forms. It can be a password, an object used as a key to unlock a technology. It can even be the inscription of a body part when used in biometric systems.

Identity verification separates authentication from authorization by granting access only when evidences and credentials have been construed as being truthful. Authorization is a set of procedures that guides how access is granted. However, there is no requirement for identity verification with authorization. Authorization is a procedural method to manage access without identity verification.

3.2.3.5 Technological Access to a Realm

The technological access to a realm is the access to the space created through technology for a variable amount of time. The technological realm is also a site of interaction. Access to this realm is granted only insofar as the identity remains verified. Access is also predicated on the level and status of the verified identity. For example, a system administrator's account affords him greater access and control over the platform than a mere user. Thus, identity verification is always in constant interaction with technological access to a realm.

3.2.3.6 Ephemeral Technology

An ephemeral technology is one where interaction with a technology occurs without apparent need for identity verification and access to the technological realm. It appears that authentication was not needed to interact with the technology. But use of technology always requires authentication. I label technologies that do not force people to perform authentication ephemeral because the identity verification and access to the technological realm occurred prior interaction at another level of abstraction. There was a prior authentication performed by a person, allowing the interaction with the current technology. Thus, the interaction with the technology is already framed as a session predicated by an authentication elsewhere. A session is transient, temporary and finite. The duration of the session is determined by the authentication that happened prior.

I refer to ephemeral technologies as water wells. As water wells, ephemeral technologies appear to be available for use without any claim to ownership enacted through authentication. For example, while traveling in the Sahara Desert with a short supply of water, I come across a water well. This water well does not appear to be owned by anyone or guarded. So, I decide to use it to refill my water reserves. This water well is a technology. It amasses ground water, allowing people to collect the water, thereafter. As I use this water well, no one has asked me for my identity and thus no one has barred access or granted me access to the resources. However, my presence in the desert was already authenticated at another level of abstraction, allowing me to use the water well.

Yet, before I entered the Sahara Desert through Mauritania, where as a non-resident, I was given access to the country through a visitor's visa where my identity was verified. The water well that I stumbled upon has been established to help travelers for decades. Although I did not need to verify my identity to gain access to this water well, authentication was performed prior when I entered Mauritania. My usage of the water well is temporary and based on my privileges given to me during my visit to Mauritania. It is a session.

So far, I have argued that the interplay between identity verification and technological access to a realm is constant, even as they occur at higher levels of abstraction. Authentication at higher levels of abstractions enables sessions to occur at lower levels. So, usage of a technology without direct authentication only means that authentication happened prior. Eventually, the interplay between identity verification and technological access ends. This makes interactions with technology ephemeral. Interactions with technology are best understood as sessions where identity verification and technological access play with one another at another level.

Without identity verification, there is no access to a technological realm. Similarly, identity verification without access to a technological realm may lead to a state of interaction nihilism. Verifying an identity without providing access provides users with no means to interact with a technology. Such information systems do exist. Users perform authentication and in exchange are granted nothing. For example, a user may log into a platform using a non-supported Internet browser. The user cannot interact with the platform even if he logged in correctly and has his identity verified. Nothing happens for him. He has no real access. One could argue that it is like inscribing one's name in a book that one already owns. No extra access, theoretically, is granted to this book. The book can already be used. It is already owned. No authentication was needed. I will challenge this premise below.

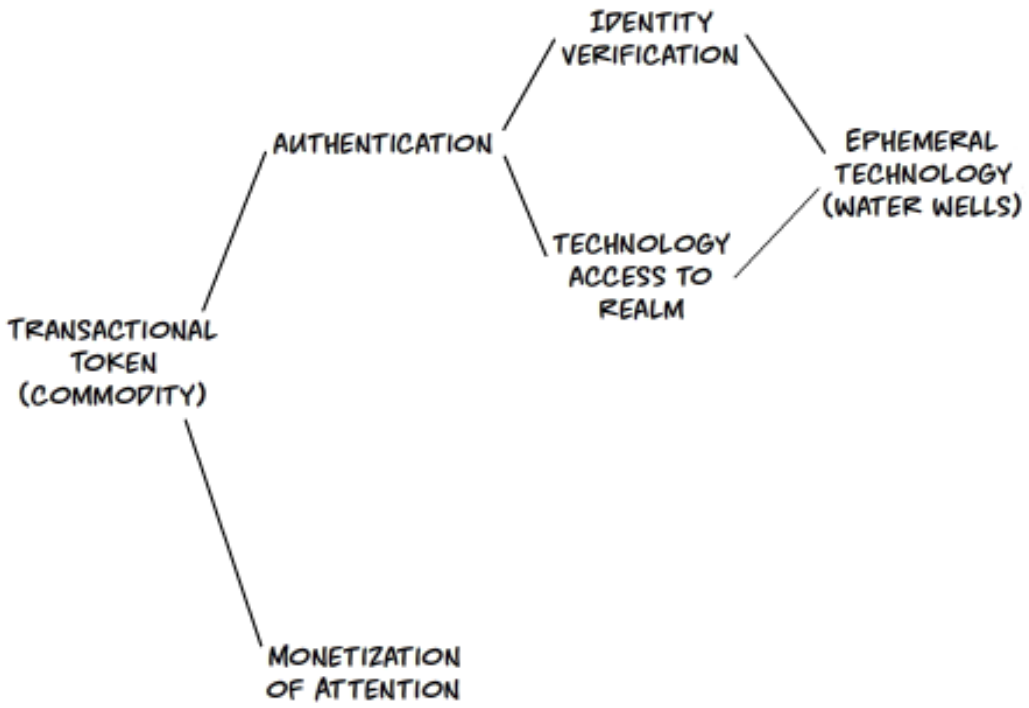

Figure 3 - Ephemeral Technology

A premise about technological nihilism leads to a question about what happens if there is no dialectic interplay between identity verification and a technological access. Using the book analogy above, one must remember that there is an underlying premise that if I can inscribe my name in a book that I own, that there was an act of ownership that preceded my name's inscription. Thus, there was a form of authentication performed prior to adding my signature to the book's front page that confirmed transfer of ownership. Similarly, if I inscribe my name in a book that I do not own, this act grants me possession (or theft!) of the book and is a form of authentication.

Signing the book's front page is not the act of authentication that matters. Signing my name in a book, until identity verification is needed, or access is contested is technological nihilism insofar as it is unnecessary. It does not mean that my interaction with the book is not ephemeral. Technology's ephemerality varies. I can keep a book that I own in my personal shelf in my home and not bother to sign my name in it. I do not need to sign it to verify my identity

and ownership or have access to it. I may never need to prove my ownership of this book through my signature, yet still have access to this book.

Technological nihilism is one outcome of an interaction with technology where there is identity verification but no access to a technological realm. An example of this is logging into a platform where the features do not work or are not compatible with one's browser or operating system. In such a state, the user cannot "do" anything once logged in. The opposite of technological nihilism is authorization. Authorization, as I have discussed above, is the access to a technological realm without identity verification. An example of this is jQuery, a public resource with usage procedures hosted on a server that any developer can link, download, and use in her own projects. When both identity verification and access to technology interplay with one another, we have an ephemeral technology. But ephemeral technologies are transient. Interaction with ephemeral technology is best understood as a session. **Table 2** displays a chart summarizing ephemeral technology, technological nihilism, and authorization. Authentication with an information system has a duration and eventually ends. Access to the technological realm and identity verification occur at a level of abstraction beyond mere usage. Technological use is one form of interaction.

Table 2 - Ephemeral Technology Model

Ephemeral Technology Model

	Identity Verification	Access to Technological Realm	Properties
Ephemeral Technology	yes	yes	Session with a technology defined by an authentication occurring at a higher abstract level of interaction.
Technology Nihilism	yes	no	Session where direct interaction with a technology occurs through identity verification. Higher levels of abstraction are not considered.
Authorization	no	yes	Session where direct interaction with a technology occurs though its usage, predicated by procedures, and rules. Higher levels of abstraction are not considered.

The use of technology, I argue, always requires authentication. Authentication is necessary for the assignment of property rights. Technology is ephemeral prior authentication and the assignment of property rights. This technology exists as part of a commons or is owned by another party who grants temporary access. Authentication becomes a reflection of ownership and nascent property rights.

So far, I have argued that the transactional token, the commodity created by tertiary authentication can be understood using a micro-level analysis that explores the monetization of user attention using sites of interaction and a macro-level investigation of authentication. Authentication and the monetization of attention are in a dialectical interplay that pits use value and exchange value. I have begun my analysis with the authentication branch of this dialectic framework.

My study of authentication is philosophical. Authentication, I argue is a dialectical phenomenon defined by an interplay between identity verification and access to a technological realm. I assert that interaction with a technology cannot occur without the constant interplay between identity verification and access to a technological realm. When it appears that there is no such interplay, we may perceive that a technology is ephemeral. Access to this technology is provisional and granted at another level of abstraction.

Ephemerality defines the state of a technology with which a person has performed an authentication. If the authentication was done at a usage level, like entering a password to have access to a platform, it is ephemeral as the session will be finite. Eventually, the user will be logged out. When logged out, both access and verification will be compromised. However, if a user has access to a technology without having performed an authentication, this does not mean that verification did not occur. Identity verification granting access has been performed at another level of abstraction.

The level of abstraction beyond mere usage is one where access and verification occurred at the property level. By property, I refer to the material entity and the rights attached to it (Munzer 2005). Authentication was granted through two forms of ownership. Either the property is already owned by the user as private property or it is part of a public commons.

This is where the dialectical model that I propose for the transactional token breaks the linear unity of proper dialectics. First, I will explore private property and continue to break this phenomenon using a dialectical approach. Then, I will explore public commons and continue to break it dialectically. The public commons branch eventually will merge with the authentication and monetization of attention branches.

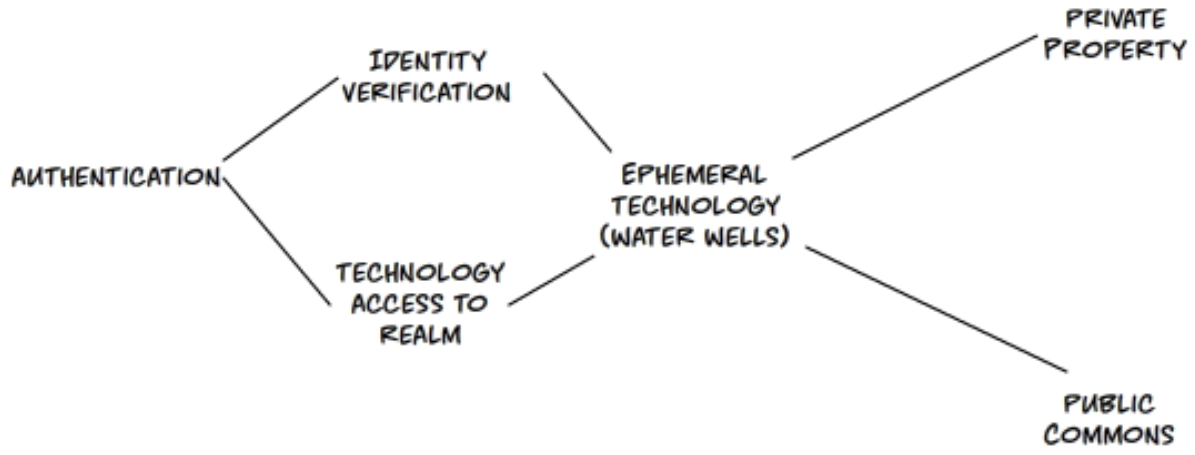

Figure 4 - Private Property and Public Commons

3.2.3.7 Private Property

Private property is a property that someone controls and has an exclusive exploitation of goods created through labour. Private property obscures the interactions between owners and non-owners. As Marx (1978) argued, private property is another way of understanding the division of labour. Marx writes that children and wives were the first slaves of the head of family (presumably the father-husband) and thus, man's first private property (1978, 151). However, the interdependence of humans to one another forced them to specialize their labour, thus further enslaving them in production roles that they cannot escape (Marx 1978).

Marx charted a history of private property where it existed in prior developmental stages in human societies starting with the power of the head of a family to dispose of the labour of other members (wives and children) (Marx 1978, 151-155). Private property coexisted in

communal forms of ownerships where clans and later tribes formed villages and cities where property was owned communally (Marx 1978).

Here, authentication plays a role in understanding the contradictory interaction between division of labour and private property. To exploit the labour of his nuclear family, the father-husband had to acknowledge and recognize these members as his own. This implicit recognition was a form of identity verification which enabled the head of the family to have access to the specialized labour of its members. Identity verification leads to access to the productive realm of family members.

The interaction between the head of the family and members of his family are analogous to the relationship between humans and technology. The human asserts her ownership over a product. While it appears to be a relationship where the subject exploits the object I do not discount the agency of the latter to change the relationship. Family members and slaves can rebel, leave, or free themselves, or reconfigure relationships.

Suchman (2007) suggested that observing interactions between humans and machines as one where one dominates the other ignored the reconfiguration that occur through their interplay. In terms of authentication as it occurs with information systems, the end-user does not own the technology. Private ownership of the technology rests with the platform operators. Often, the user owns the physical object but not the software or the platform used to exploit the device.

I argued above that ephemeral technology is just technology where authentication has been performed at another level of abstraction in the form of private property or public property. To understand where this comes into play let us return to the water well example found in a desert. If you stumble upon the water well in the desert its ownership is either in the form of private property or as part of a public commons. The apparent level of abstraction where the water well appears to be an ephemeral technology where no authentication to physically use it is a cover.

If the water well is private property, access will be granted through the intermediation of its owner. This exchange is a form of authentication. The weary traveler will have to be verified,

perhaps through an exchange of commodities, or money, or be granted access before having access to the water from the well.

However, if the water well appears to be part of a commons, access may be granted because the weary traveller is recognized as having the right to be in the place where the water well is located. Access is granted through the verification of the traveler's identity as constituting the necessary right to be near the water well. Even access to public commons requires identity verification to have access to a realm.

Access to the water well does not prevent subsequent forms of authentication to occur at the exact site of interaction. Being in the desert means that the traveler has been granted access to a territory that may be the private property of one owner or the public commons of a larger group, or an institution. Authentication occurred before the traveler reached the water well.

Another example is a non-student having access to an academic library. In this example, the academic library is both a private property as it is owned by the university and a public common good as most university espoused traditions and values of open access to the public. In this example, it is presumed that anyone can enter an academic library. But is that so?

First, to be able to have access to the academic library, visitors must be able to travel and be near the building, or as I prefer, the site of interaction. A foreign national who is not allowed in the country where this library is located will not have access to its collection unless he has been authenticated to be in the host state. The identity verification and access to the realm where the library is located were granted to the foreign national at the border.

If the foreign national attempts to check out a book from the academic library, another round of authentication will be performed at the site of interaction. To have access to the academic library presumes that the visitor's identity and access have been granted at another level of abstraction. In this case, access to country grants access to the academic library.

In the case of an information system, like access to a platform like Facebook, there is a presumption that the visitor has been granted access to a computer, first, and then the Internet at different sites of interaction. This is way of understanding interaction is adapted from Internet

founder and researcher David Clark's (2012) control point analysis. While Clark used this method to map the different point of control that users faced as they used the Internet (2012), I chose to expand this method to explain how people interact with technology at different sites.

Clark's control point analysis describes every potential point of external control over a user navigating the Internet (2012). While he created control point analysis to measures possible places where surveillance and deny of access to an information can occur, this method is useful when surveying user's information practices when interacting with information systems.

Control point analysis has not yet been adopted in human-computer interaction, usability, and user experience studies. This method offers simple ways of conceptualizing design models but also rests on an evaluation that considers all steps that a user must perform before completing a task (Clark 2012). This includes starting a computer, enabling Internet access or performing an authentication into a desktop computer (Clark 2012). Architectural variables that affect user interaction such as packet switching and the three network levels of the Internet network backbones, the level of regional and local Internet services, and individual vertices of ordinary computers (Newman 2010) are considered in control point analysis (Clark 2012).

Marx argues that private property has changed as it has had a continued existence with competing forms of ownership such as communal property, feudal property, or corporatist property (1978). One change has been the codification of property rights which has forced private property to exist and justify its being through codification as opposed to practice. This codification of property rights into law was a result of the 17th century Enlightenment and a process of gradual restrictions state power and sovereignty (Lindsay 2005) against civic elites in Europe (Marx 1978).

The legal codification of private property exposes new dialectic contradictory strategies about the nature of authentication that I will explore next. Private property exists in a context and environment where property rights are not absolute and must be conferred by a higher authority (or level of abstraction). They are enfranchisement and what I define as timesharing.

3.2.3.8 Enfranchisement

I borrow the term enfranchisement to describe the practice of curbing state power by extending property rights. Traditionally, enfranchisement is related to civil rights such as the right to vote (Munshi 2010). Collective enfranchisement is another way that the term has been used in British law to describe collective leases of home properties (Smith 1994). Here, enfranchisement is a limit on authority's control over individuals by fabricating a *zone franche*, a space where rights are assigned to citizens by the state. It is also an absolution of servitude of the subjugated. Rights produced include newer rights such as privacy, and the universal vote, and older rights such as a limit on state seizure of property and open-ended search warrants (Lindsay 2005). The nature of the enfranchisement depends on the ideology of the dominant class in society, as argued by Marx (1978, 163-174).

Enfranchisement is a form of authentication for the individual allowing him through state verification to obtain a legitimate claim to exploit and access a resource. In the context of authentication and information systems, enfranchisement is analogous to copyrights. In copyrights, authors, artists, and musicians engage in production of goods whose ownership is guaranteed by the state. The state can limit the scope of copyrights or extend it although an individual produced a work. Copyright laws settle claims by verifying the identity of the producer and grants her exclusive access to her production.

Similarly, enfranchisement grants users access through identity verification to exclusive products. Platform operators operate within legal frameworks be they state-based or based on para-legal protocols found in many Internet technology protocols. Having secured enfranchisement, platform operators can resell access to their platforms to their users. However, enfranchisement is a utility not a means of exchange. Timesharing is the how access on a private property is exchanged.

3.2.3.9 Timesharing

Timesharing is an alternate term for shared computing, a concept that I described in the literature review drawn from the history of computer sciences. Timesharing in computing evokes the period of the 1960s and 1970s when several users, often in universities had scheduled

sessions when they would share one computer in a laboratory. In this framework, timesharing is how private property is exchanged during authentication. Timesharing is a temporary reprieve given to an individual at the site of interaction. People timeshare space on platforms but do not own them. Their data can be remitted or exchanged. The data they own is part of their labour on the platform but not all part of this data i.e., metadata is owned by users.

Earlier, I argued that ephemeral technology reflected aspects of authenticated sessions, where users access technology (or a space) while having their identity verified. Timesharing appears to be similar but for the fact that people are aware that they are interacting at a site of interaction. Ephemeral technology is one where the user has been authenticated prior on a higher level of abstraction. Timesharing occurs at the level of abstraction of the information system. The ownership of the information system is private and therefore only guaranteed through the state.

An important aspect of timesharing in the context of this study and the information economy, is related to economic theorems. Timesharing, like other practices evolving from the development of information and communication technologies (ICTs) appears as a new economic contradiction. Economist Yann Moulier Boutang (2008) argues that many economic theorems are contradicted by phenomena and practices stemming from the information economy. For example, he argues that copyright laws and legal frameworks have difficulty to adapt their controls over the reproduction and valorization of digital goods which easily escape the exclusive distribution schemes of contents producers.

Marginal costs associated with the hosting of users' data are minimal (Moulier Boutang 2008, 160). There are two types of marginal costs to consider. The first are marginal operating costs, which are the costs platforms incur as they serve one additional user (Shy 2008, 53). For example, this is the cost that Facebook must absorb when a person joins its platform. The second are marginal capacity costs. These are the costs platforms absorb when they host user data on their servers (Shy 2008, 53). For example, this is the cost that Google incurs when it hosts the data of one user on its platform. Marginal costs for platforms such as Facebook, Google, and Twitter are minimal.

Scarcity is a second apparent contradiction that is inherent in timesharing. Scarcity is a classic economic theorem where the needs by a multitude for the same finite resources increase the demand for the latter, and thus makes its availability scarce (Burke 1990). In the context of privately-owned platforms, scarcity is the amount of resources needed to store users' data on a finite number of servers. Scarcity is related to the marginal operating cost since platform operators must constantly assess and protect user's data on their servers. Scarcity is also associated with marginal capacity costs. Platform operators must constantly manage and allocate space to users on their servers. The cost of securing users' data is part of the costs related to scarcity, marginal operating costs, and marginal capacity costs that platforms bear. Users can add unlimited data to platforms without easily reaching the servers' capacity. Scarcity seems a distant concern, and thus the second contradiction stemming from timesharing.

Twitter demonstrates the effect of scarcity best. Twitter constrains the expression of tweets to 140 characters. This is not scarcity that originates from market forces, unless one accounts for Twitter's differentiation strategy as platform. This scarcity is imposed by Twitter. Yet users can post multiple tweets if they wish to. Twitter still has a limit on the number of tweets users can post daily or how quickly they can post them. But what is more telling about scarcity are the problems that Twitter, as a timeshared site of interaction faced in its early years. Twitter was plagued with scalability problems that often led to the platform lacking the resources to serve the needs of its growing audience. The 'fail whale' was a cartoon image of a whale that users saw when Twitter faced outages. While Facebook, Google, and Twitter appear to function smoothly and to have unlimited resources, making scarcity almost hypothetical, this is not the case for most platforms. Several rely on cloud-based resources from merchants such as Amazon. They have finite resources. It is only with scale and more market and architectural proficiency that platforms such as Twitter could escape their scarcity challenges and appear to have unlimited capacity to sustain timeshared technologies.

Yet I maintain that marginal costs and scarcity challenge economic theories but are not contradictions as defined by Moulier Boutang (2008). In the traditional definition of timesharing, users would rent space on a timeshared property like a vacation condo to gain access to space (resources), and time on a private platform regardless of what they may produce at the site of

interaction. In other words, the data a user generates on her Twitter account while appearing as her own is still used through a platform whose ownership she does not possess. Twitter, as a platform operator, can still claim some of the data produced by its users. Often, platform operators will grant themselves the right to use user-generated data without making a complete claim of ownership to the product.

Just like a timeshared property such as a vacation condo, users rent space (resources), and time on a private platform regardless of what they may produce at the site of interaction. In other words, the data a user generates on her Twitter account while appearing as her own is still used through a platform whose ownership she does not possess. Twitter, as a platform operator, can still take some of the data produced by its users. Often, platform operators will grant themselves the right to use user-generated data without making a complete claim of ownership to the product.

The correct analogy is not the timeshared condo but the digital sharecropping analogy proposed by scholar Nick Carr (2016). In Carr's analogy, users can produce and grow content on platforms but at any moment, platform operators can take the generated data away. The production of data by countless hordes of people on platforms adds value to the latter.

My theorization of timesharing starts setting some of the processes that lead to the commodification of user data. Both timesharing and enfranchisement are aspects of property rights. However, to fully explore property rights as they relate to authentication, I must return to the public commons which was mentioned above as a branch that split from ephemeral technology earlier in the framework.

3.2.3.10 Public Commons

The public commons are a level of abstraction beyond the ephemeral technology where authentication occurs. Unlike private property, the public commons are a space (technological or not) where access is not based on individual ownership or property yet requires authentication through the recognition from a community of practice or a guarded technology.

An example of a public commons is a national park. Travelers can visit and often even camp in national parks. However, access to this public good is provided to all residents of a well-defined space as part of rights of access verified through implicit membership. That is, to visit a Canadian national park, for example, Canadian nationals and residents can easily gain access to the protected area by providing their citizenship verification. They also pay taxes at other levels of abstractions which verify their identities and grant them access. The taxes are not fees paid to an individual or a firm. They are paid by all residents to a national government. Children who do not pay taxes, implicitly have their identity verified through their legal guardians and still have access to the resources.

Visitors can also have access to a Canadian national park but their access has been granted through prior access to the country. Identity verification that provide access to public commons is not done through enfranchisement or timeshare as with private property. It is done through recognition of community of practice and through guarded technology.

3.2.3.11 Guarded Technology

While recognition through community of practices is related to property rights, as enfranchisement and timesharing, guarded technology explores another branch about human interaction with technology. A guarded technology is a public and secured technology where identity verification and access are performed through by a lack of availability. Authentication with this technology is performed through exclusivity as it is withheld from circulation. A guarded technology is a protected technology that is withheld from circulation and only available through an exchange or accumulation[8]. Few individuals have access to guarded technologies. Access to them is exclusive.

An example of guarded technology is the early computers of the 1950s and 1960s. There were no passwords or overt authentication methods to access these computers. Authentication, as noted in the literature review chapter only occurred when multiple users had to share computers

[8] The definition for the term accumulation differs from Marx's definition. This is discussed below.

in one single environment. Because the computers were not in circulation, they were not available for public use even though they were public goods.

I explore how guarded access to guarded technology occurs below. Guarded technologies are available only through technology exchanges or accumulation. I explain these two terms below in the context of the transactional token framework. Before doing so, I explain the other dialectic branch stemming from public commons which starts with a discussion on recognition through communities of practices. This branch merges back in to the property branch mentioned earlier but that has not been explored fully. The property rights branch continues the dialectic approach until it reconciles back into the larger transactional framework.

3.2.3.12 Recognition through Community of Practices

Communities of practices is a social theory developed by Étienne Wenger (1998) that sought to explain how groups learn through practice and constant interaction. In communities of practices, peers learn from one another and shape common cultures and practices as defined by their networks. Original computers were shared commons within a community of practice.

I argue that one way authentication in public commons is performed is through the mutual recognition of peers through communities of practices. Authentication is performed through human-to-human interactions. Tacit access to public commons is granted through familiarity or other forms of interactions. These interactions are predicated through social and techno-material structures.

To reuse my example of the water well and public commons, authentication in such a setting could be provided through the recognition of other members of a tribe of one of their own. Hence access to the well would be granted based on familiarity. The public commons are shared by a group or an institution that quickly recognize on of its own and grants her access to a realm.

I claim that recognition through a community of practice can be performed through interaction schema involving humans. But what about the case of a hacker that finds the right code to interact with a technology and succeeds in hacking it and gaining access to its

technological realm? Is deciphering an encryption not a tacit way of dialoguing with a peer, using guile and technological means?

Communities of practices in this model develop around shared technologies. Hacking is not about using a peer-based shared technological realm. While often deriving from public commons, they can be private resources too. A family computer to which no login has been set, for example, can be used by all family members. No one would question such usage.

Similarly, an office printer used at a workplace and which is available without having to perform any authentication at the site of interaction is a similar technology part of a public common. Anyone in the office plugging a USB cable from the printer to their computer would not draw any attention from other people in the office.

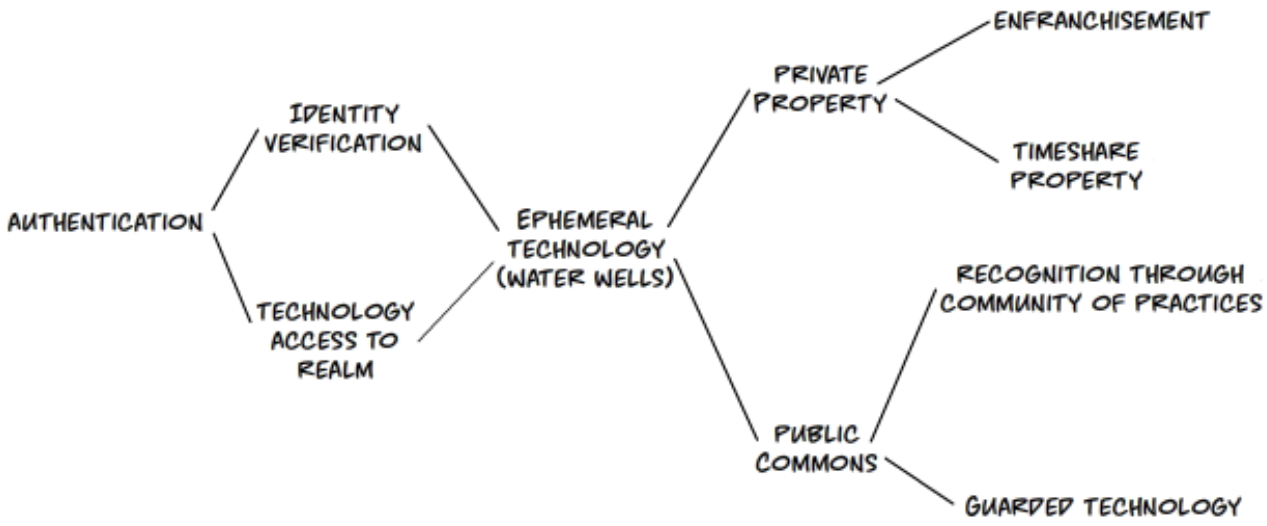

Figure 5 - Expanded Private Property and Public Commons

3.2.3.13 Property Rights

Recognition through community of practice presupposes that ownership is held communally. Communal ownership is a type of property right just like enfranchisement and timesharing. Property rights limit intrusions, seizures, and threats from the state and non-state intruders (Nissenbaum 1997). In the early industrial and modern age, property rights protected the bourgeoisie and the nobility from state power intrusion.

The property rights obtained by land elite and the bourgeoisie before the industrial revolution have changed and become universal in the information economy. Rights such as privacy only merited serious philosophical discussion in the 1960s as a reaction to improved government surveillance capabilities and major court case challenging state intrusions in the United States (Lindsay 2005). While authentication has become an important means to secure property rights at lower abstraction levels it is also inherent as a form of interaction at higher levels of abstractions. The enactment of property rights at the individual level occur through acts of authentication. A license is a contract that provides both verification and access to an individual to a realm apart from others.

While some rights are more outward-looking and progressive, like democracy, fraternity, and liberalism, other rights, especially in the information economy are more inward-looking and defensive in nature. [9] While progressive rights encourage what one can be and what one can do, defensive rights protect what one is and what one possesses. Authentication reinforces this and is inherent in the practice of defensive property rights such as privacy and security as will be seen below.

3.2.3.14 Privacy

As argued in the Chapter 2's literature review, privacy as a phenomenon has been difficult to define. In the context of the transactional token framework privacy should be understood as a property right allowing the individual to control information about one's self. It protects what one is.

[9] My taxonomy of outward-looking (progressive) and inward-looking (defensive) property rights varies from the concepts positive and negative rights found in political and legal theory. It is closely related but not an exact match. Positive rights are based on state actions that enhance citizens' rights (Currie 1986). Negative rights are those where individuals are protected from the coercive actions of the state (Currie 1986). My usage of progressive rights is not dependent on the state to act to enhance and protect citizens' rights beyond the codification of rights. Progressive rights are dependent on individuals' agency, not structures like the state. Defensive and negative rights match more closely as each is about preventing state coercion. One difference between defensive and negative rights as used in the transactional token framework, is that the former focuses mainly on property rights, not all human rights. Hence, progressive rights address human rights where defensive rights address property rights.

Privacy can also be the protection of what one possesses to the extent that property can tell a lot about its owner. In terms of data and information, it can even leave a trace such as meta-data that can be analyzed to understand the individual behind.

3.2.3.15 Security

Similarly, security is a property right which as noted in the literary review chapter, is often thought to encompass aspects of privacy. Security is a property right allowing individuals to protect the integrity of objects but also their personal safety. Hence security protects both what one possesses and what one is.

While covering one aspect of property right more than the other, security and privacy overlap and both protect in a usual dialectic contradiction who the person is and what the person possesses. Taken together these two properties reveal much about an approximate person which is more identity than human.

3.2.3.16 Identity

Identity is the space created around the person to protect property rights but whose attributes or lack of, define the protected, creating a documented public self and a private self. The documentation of identity is a form of registration and something that can be exchanged. This identity is created at the site of interaction and therefore is part of the authentication produced by users interacting with an information system. The data about the identity of users, allowing them to authenticate into an information system is exchanged with individuals in the form of user tokens, pieces of data that people keep with themselves a key to unlock an information system. Third parties also have access to this data through application programming interfaces (APIs). Scholar John Cheney-Lippold (2011) refers to any digital traces left behind by a user and used by a third party as part of an algorithmic identity (Cheney-Lippold 2011). This identity, presumably does not require people to be logged in. However, as I argued above, there are two levels of authentication that people go through. One is conscious. The person logs in. But there is an abstract level beyond the ephemeral technology where users have already performed authentications with the systems that they use before they ever enter a password in an entry box.

Users and their identity are not the same. One is a subject, the other an object about the subject. Through authentication people create identities that can be commodified. User-agency, as I argued earlier in this chapter is inherent while they perform authentication. But this agency is limited as it allows platforms and third parties to verify users' identities. Users can obfuscate the information they provide and create fake or approximate identities. However, even these obfuscated identities can be commodified by platforms. The information provided by users can also be matched with metadata generated during their interaction with information systems. These are also generated during an authentication and are added to the overall identity collected about people.

3.2.3.17 User Token Generation

Think of user token generation as the process of creating a password that is used as a key to unlock a closed information system. People must create a token for themselves that is used to perform the authentication. Passwords remembered or inscribed on a piece of paper, memorized patterns, or images are also user tokens. There is another form of user token which is generated or transferred to people, like fob keys. Fob keys are usually handed to people. Users do not decide the exact code that is used to allow authentication. Another form of user token can be generated by the digitalization of information taken from users, like biometric data.

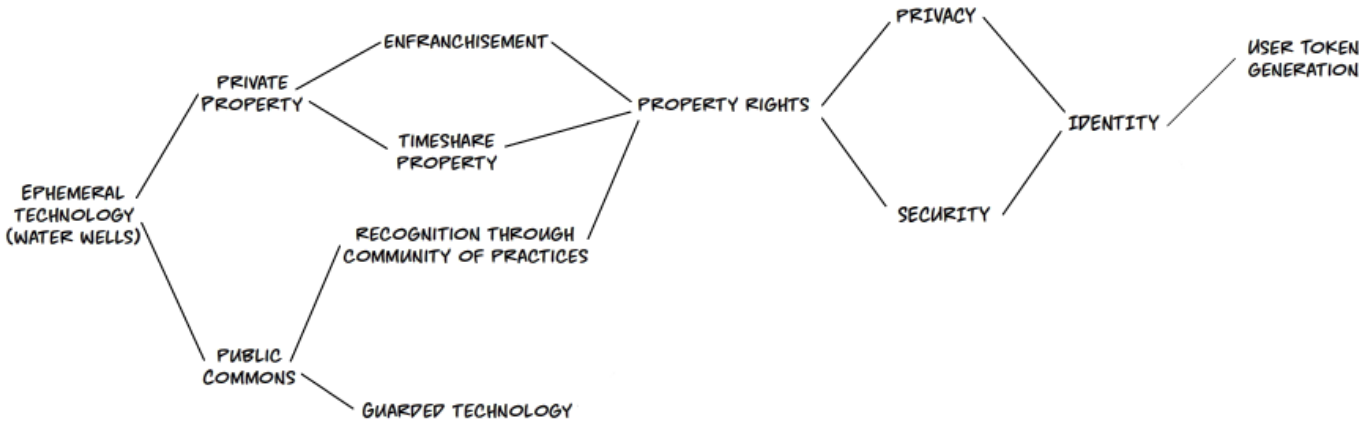

Figure 6 - User Token Generation

Before going forward, I will go back to the guarded technology branch that was introduced earlier. This branch is parallel to recognition through community of practice which also sprang from the public commons.

3.2.3.18 Technology Accumulation

I argued above that public commons are spaces where authentication occurs on another level of abstraction beyond the instrumental authentication into an information system. It occurs in two ways through peer recognition, or what I termed community of practices, or through guarded technologies. Guarded technologies are withheld from public use. Guarded technologies' access is exclusive and limited to a few individuals. Those individuals have access to them through technology accumulation and exchanges. Let us look at technology accumulation first.

Accumulation has two meaning in classic Marxist theory. The first is primitive (or primary) accumulation. Primitive accumulation is the process of expropriation of small land owners in early capitalism that led to a surplus of workers that had to sell their labour to subsist (Marx 1992). The other form of accumulation discussed by Marx is capital accumulation. Capital accumulation is the process through which capital is accumulated through the dependence on worker's labour to accrue wealth and the control over production. Workers become necessary to increase the accumulation of wealth while they do not control the means to generate this wealth (Marx 1992). My definition of technology accumulation draws on some principles of primitive and capital accumulation but is not a direct analogue or use of the two Marxian terms.

Technology accumulation here does not attempt to make a parallel between workers and their relation to capital with users and their interaction with technology. Instead, I use the term accumulation to describe a guarded technology whose access is exclusive because it is still being produced or changed before being released publicly. I use the term accumulation in the sense that production of a technology is involved but its circulation is restricted. Circulation, again, does not borrow the Marxian definition of the term whereby commodities are exchanged and transformed. Circulation here describes the availability of a technology to users.

Technology accumulation is another form of authentication that occurs on an abstract level of interaction. For example, the production of the release of a beta image editing software whose availability is restricted to the developer and a few beta testers is an example of technology accumulation. The developer and the beta testers must perform authentications to use the technology, even in its unfinished state. Formal authentication schemes are not necessary. The application's developer and beta testers have access to the technology and have been verified because they are the ones producing it. However, in some development platforms such as Apple's iOS, developers and beta testers must formally authenticate themselves on the devices that they use before they can access their own in-development apps.

Another characteristic of technology accumulation is the destruction of technology. Economist Joseph Schumpeter (2013) discussed a type of destruction that occurs in capitalism which he coined creative destruction. Creative destruction is the process through which new forms of economic organization destroy older forms from within. Improved class of industrial goods like mobile phones make older versions irrelevant (Schumpeter 2013). For example, the smartphone has made older mobile phones devoid of computers uncompetitive.

Creative destruction is echoed in my coining of destruction as part of technology accumulation. Accumulated technologies are produced for consumption and appropriation. The production of accumulated technology, comes from new development of technology or its destruction. The developers and the beta testers developing the technology have exclusive access to it as they forge it. They are its producers. But technology accumulation can also be obtained if it is corrupted, hacked, or pirated. This is the destruction of technology. New producers change the original image editing software into a new rogue version that compromises the integrity of the original version. From the point of view of the legitimate and original producers of the image editing software, the thieves, the hackers, and the pirates are unauthorized users of this technology. However, by changing parts of the code within the software, these new producers have performed an authentication into the program. They have appropriated a version of the software or in the case of a platform or a website, the version running publicly. They have creatively destroyed the older information system. Yet the actions of these new producers, before they hand over the software to the public is still an exclusive act of ownership. Authentication

happens on an abstract level which means that whether they need to enter a valid or fake identity to have access to the appropriated information system, they still performed an authentication by transforming the original product.

In practice, the production of a technology may involve a dialectical process of development and destruction. The consumption (by its developers and legitimate users such as beta testers) and appropriation (by thieves, hackers, pirates, and limited numbers of users of pirated software) of technology runs in a dialectical process against its production. It involves the theft, granting, taxation, or the reproduction of a technology. A technology can be copied against the wish of it owner; it can be granted or given away, like free software; it can be obtained through taxes, as a form of commodity; or it can be reproduced.

3.2.3.19 Technology Exchange

Guarded technologies need to be exchanged to be used by users. This exchange is another form of authentication. The purchase (by a user) and sale (by a platform operator) of licensed items are the most common forms of exchange of guarded technologies. The exchange of technology happens against another commodity. Here, the technology exchanges take us closer to the act of commodification that happens when a user creates an account to have access to a technology. With some technological exchanges, the purchase of a technology, or access to it replicates the dialectic process of verification and access that is central to authentication.

Different commodities can be used to obtain guarded technologies. Commodities include money, but also labour, such as crowdsourcing or collaboration on open source software. There is a process of access to technology through verification that authenticates participants to crowdsourced software projects. People's identities and personal information is not part of the commodities used in the exchange. At this stage, there is no commodification of people's personal information. To obtain the technology, the user must sell another commodity.

3.2.3.20 User Licensing

User licensing follows technology exchanges and accumulation. The license obtained by the user confers a form of authentication to a single instance, in most cases of a guarded

technology. User licensing is the reselling, the renting or the licensing of an exclusive guarded technology by a technology owner or operator to end users and third parties. User licenses provide people with authorized access to technology through a process of verification of their credentials. It is also the first step of commodification of the user's information as a separate contract binds her with the operator of the technology.

The license is also a documented token kept in confidence by the platform operator about users of its technology. I explore below how user licensing connects to data exchange, which is one area covered by the monetization of attention branch that I left behind when I started my discussion of the authentication as one of the two dialectical foci of the transactional token.

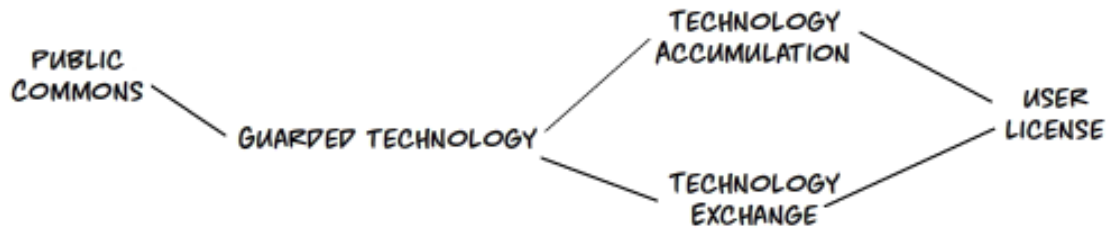

Figure 7 - User License

3.2.3.21 Monetization of Attention

The transactional token framework that I have introduced has explained authentication using a macro-level and philosophical approach. I started by exploring the dialectic aspects of identity verification and access to technological realms that characterize authentication as the creation of ephemeral technology. Ephemeral technology reflects aspects of authenticated and transient sessions where users access technology (or a space) while having their identity verified. But as I argued, an authenticated session, or ephemeral technology hides the fact that prior authentications occurred first on another level of abstraction. The ephemeral technology is only possible if one accounts that authentication was performed either through private property or public commons before an authenticated session with one technology. Private property provides exclusive exploitation to its owner or operator. Being a private property, access was granted to the owner/operator through the state. But private property is only possible through a process of

enfranchisement where limits are put on the state allowing a free zone where the technology can be developed. Timesharing is another type of transient use of technology where users, through their labour can add value to a technology yet do not own the platform that they use. Unlike ephemeral technology, the authentication with the timeshared technology is at the same level of abstraction of users interacting with the technology. Enfranchisement and timesharing are aspects of property rights.

Public commons, unlike private properties are the space where authentication in one technology is predicated by having access to a public good first. But public commons also require authentication through communities of practices or through guarded technologies. Guarded technologies are technologies in the public commons whose use excludes to the public. Authentication to guarded technologies occurs through technology accumulation and technology exchanges. Technology accumulation is the production of technology or it subversion through destruction. Technology exchange trades a guarded technology against another commodity. Communities of practices are a peer or community-based level of authentication of individuals using a technology.

Property rights are established by societal elites who own the means of production to protect their rights from encroachment from the state. They can be progressive, like fraternity, democracy, liberty; or they can be defensive and protect what one possesses. I have argued that security and privacy are property rights that have gained more prominence in the information economy. These rights make use of authentication processes to protect the identity of people in the information economy. While the person desires to protect its identity as it uses technology, technology accumulation and exchange create another form of identity for people in the form of user licenses held by technology owners and operators. User licensing merges back into monetization branch. I will come back and finish exploring user licensing, identity, and authentication but to do so, I must first demonstrate the monetization of attention.

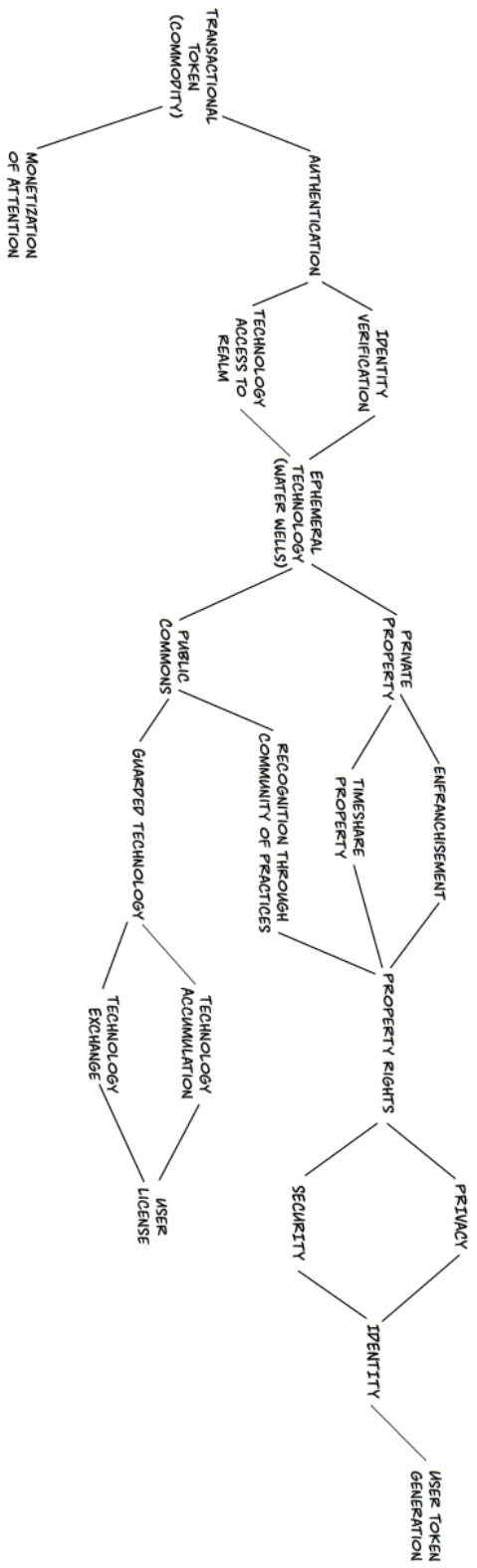

Figure 8 - Authentication

I intend to explain the second part of the transactional token framework by focusing on the monetization of attention branch using a micro-level analysis that just like the authentication branch is grounded by control point analysis and a focus on sites of interaction drawn from human-computer interaction literature. I propose a micro-level analysis of every step that leads to the commodification of audiences' attention, once they perform an authentication with a platform. Attention is a form of interaction but also labour.

I argue that a dialectical process characterizes the interplay of various processes where contradictory propositions are often resolved with a new thesis that reveals subsequent contradictions and processes. Parts of the monetization of attention branch merge with other sections from the authentication branch and ultimately, both branches reunite at the end. The monetization of attention is about the exploitation and the commercialization of user interaction with platforms in the form of user financing, subscriptions, or advertising.

Lee (2011) identified three types of advertising commodities that are fabricated and maintained within search engines ecosystems like Google's. They are keywords, ratings (or statistics), and search results (Lee 2011). From its narrow focus on search engines and search engine advertising, Lee's triad of commodities can be adapted to cover much of the types of commodities generated by platforms beyond search engines.

Keywords, according to Lee are more important than demographics in determining which ads appear in front of audiences (2011). Keywords are preponderant in search engine advertising, including that of partner websites in Google's AdSense network. While keywords are one metric, what they really reveal are the interests and themes sought and shared by audiences. Interests and themes can thus cover more ground than keywords when it comes to understanding one of the commodities used by platforms such as Facebook and Twitter which are not directly search-based.

Ratings are the other metric used by search engines like Google, according to Lee (2011). Ratings provide quantitative data on the advertising effectiveness and performance of keywords but also on the demographics of users. Ratings also encompass the traditional broadcast data of audiences (Meehan 1993). To make ratings relevant to platforms it is important to understand

that they can be interpreted as user statistics and metadata. Platforms such as Facebook measure a wide range of metadata generated by users and use them to better understand them (Facebook 2015).

As well as measuring overt information such as age, gender, education levels, and religion, Facebook also measures how long users preview content such as videos, what posts they react to, and even what they avoid (Gomez-Ortigoza 2016). These are metadata about user usage of the platform. Other platforms, to some extent also monitor such metadata. For example, Amazon suggests to shoppers, products based on previous purchases; Netflix suggests movies and television series based on previously viewed contents.

Finally, Lee proposes search results as the last metric used by search engines (2014). Again, I expand this to include analogous commodities found in other platforms. Search results are contents, but they are better understood as part of an experience. More than the successful task completion involved with search results are people's perceptions and feelings as they perform searches (Albert and Tullis 2013). Content limits search results and others such as a chat session on Facebook Messenger or a timeline of tweet do not completely explain what is happening and accessed by people using platforms.

As argued by Hassenzahl (2008), there is more to users' interaction with information systems than seeking a product, a specific content, or achieving a goal. The experience of interacting with a platform has hedonistic qualities that are sufficient motivations for people (Hassenzahl 2008). For example, seeking new followers or increasing the number of likes on one's posts has a hedonistic quality even if information seeking behaviour is involved. Therefore, I prefer using the term experience to denote the hedonistic pleasure and satisfaction that people derive from their interactions.

User financing and subscriptions are two other forms where users' attention can be commodified by platforms. User financing can take the form of crowdfunding or other financial operation where people directly fund other people, products, services, projects, or even a platform while having authenticated themselves. This can include a person shopping on Amazon, bidding on eBay, crowdfunding on Kickstarter, or buying ads on Google AdSense. Subscription

is similar in that users register to obtain a service or a product on a platform. This can refer to people subscribing to the online version of a newspaper or a magazine, funding a project every month through Patreon, or having a subscription to an enhanced version of a social network like LinkedIn.

In both user financing and subscriptions, platform operators are involved in commodities such as interests and themes, user statistics and metadata, and experiences generated through people's interactions. However, in the transactional token framework that I am introducing, user financing and subscriptions will not be addressed further. Still many of the interactions involved in other forms of monetization of attention can apply directly to user financing and subscriptions. The monetization of attention at this point is still an abstract concept. Its operationalization happens in a dialectical process through hit views and response to calls to action.

3.2.3.22 Hit View

In Internet statistics' vernacular, a hit is any time a request is made to a server regardless of whether an actual person viewed the page or accessed it. For example, a link to an image on a website from a third party will create a hit on the original site regardless of whether anyone saw or accessed the image. I use the hit view analogy to explain the total interactions with the information system including those that originate from humans, machines, randomness, and error. People are exposed to many possible ads and prompts from marketers and platform operators but only react to some of them. Some interactions performed by users are invisible and unknown to them. Hit views are problematic for platforms, advertisers, and other data aggregators. They can produce results and data that are perceived as illegitimate and a deceitful representation and account of an audience because they measure everything. Advertisers and data aggregators are interested in audiences mainly.

3.2.3.23 Call to Action Response

A call to action response is a user-based interaction with the information system where engagement has occurred. The user performs an action encouraged by the platform and its advertisers satisfactorily. Unlike the hit view, the user is a willing participant in the interaction with the information system, once they have authenticated themselves. The two kinds of

interactions can occur at the same time. These interactions occur as users seek, use, and share information on a platform.

3.2.3.24 Advertising Interaction

Hit view and responses call to action are advertising interactions. An advertising interaction is a monetized interaction with an advertisement renting space within an information system. Users have three types of responses when interacting with advertising. They can resist (resistance), interact with the ad erroneously (error), or buy-into the prompt (buy-in) they receive from the advertisement. Let us look at these three types of user responses to advertising interactions.

3.2.3.25 Resistance

Resistance is the first type of user response to advertising interaction. Users do not react positively to every monetization and advertising prompts in a way that benefits platform operators or marketers. Users can actively seek to block advertising interactions. User resistance to advertising and monetization can take multiple forms such as opting out of interests-based ads, suppressing ads, stop noticing ads, or just avoidance of advertisements.

3.2.3.26 Error

Error is the second type of advertising interaction. Error is a user-based interaction with an advertisement where a fault is involved. For example, the interaction with an ad may be involuntary, as a cat stepping on a keyboard.

3.2.3.27 Buy-In

Buy-in is the third type of advertising interaction covered in the transaction token framework. Buy-in is an interaction where a user responds favourably to an advertisement while authenticated. Transactions do not have to be fulfilled. Users can abandon them at any point.

3.2.3.28 Data Generation and Aggregation

Data generation and aggregation occurs once users' interests, themes, user statistics and metadata, and experiences are collected through the platforms. This includes in

better platforms, data from user resistance, error, and of course buy-in. Data from resistance and error may be as valuable for platform operators as buy-in data. In fact, some of it may be discarded and ignored, or used to design a commodified user's profile.

3.2.3.29 Data Discarding or Ignorance

Through influence and imperatives, platform operators decide which data gathered from users' interactions is valuable or not. It is likely that platform operators try to keep as much data about their users as they can by law but ignore that which will not support the commodification and targeting of audiences. It is also at this point that much of the unnecessary data obtained from hit views is discarded.

3.2.3.30 Design & Profiling

Design and Profiling are about the redesign of the information system based on user interaction and creating data schemes around information gathered from user interaction. Platforms' operations and constitutions are part of an iterative process of redesign and optimization so that features best match the intent of operators and sometimes, users. User profiling is part of a similar process of reinvention to constantly allow operators to have the best grasp of audiences.

3.2.3.31 Targeting

Data discarding, ignorance, design and profiling are dialectic processes that lead to audience targeting. Targeting is important in the process of commodification of audiences' labour. Users' prior data is used by platform operators to better target them with monetization schemes. Here, I want to differentiate design and profiling from targeting. Design and profiling are practices where user data is manipulated. Targeting is the use and application of the data that was manipulated by platform operators. Targeting is about the use of data that has been enhanced through data discarding, ignorance, design, and profiling.

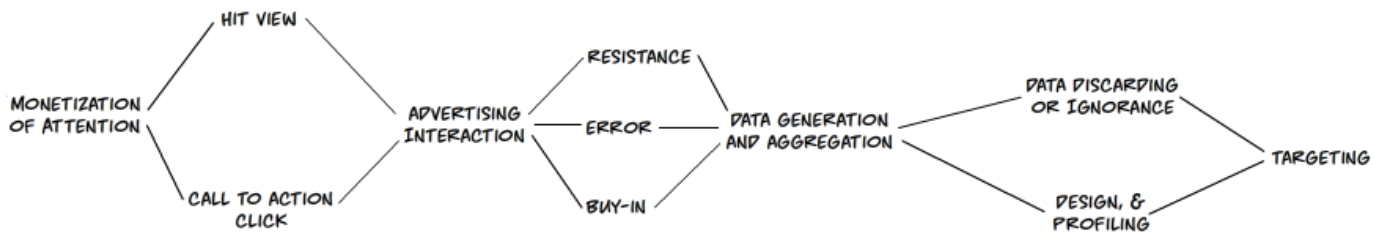

Figure 9 - Targeting

3.2.3.32 Data Exchange

Data generated from user targeting is exchanged with third-parties as a commodity. However, data also generated from user licensing is also exchanged with third parties. Data exchange is the full commodification of data obtained from users. There are two types of third parties with whom data is exchanged. The first are third parties with access to APIs generated by platform operators for third-party developers to allow authentication of their users with tertiary applications. The other third parties are advertisers who gain access to data generated from user licensing or targeting. Licensing and targeting differs in that with the former, data is obtained from the transaction of the user acquiring a technology of his use. In targeting, data is obtained from user's interaction with a technology.

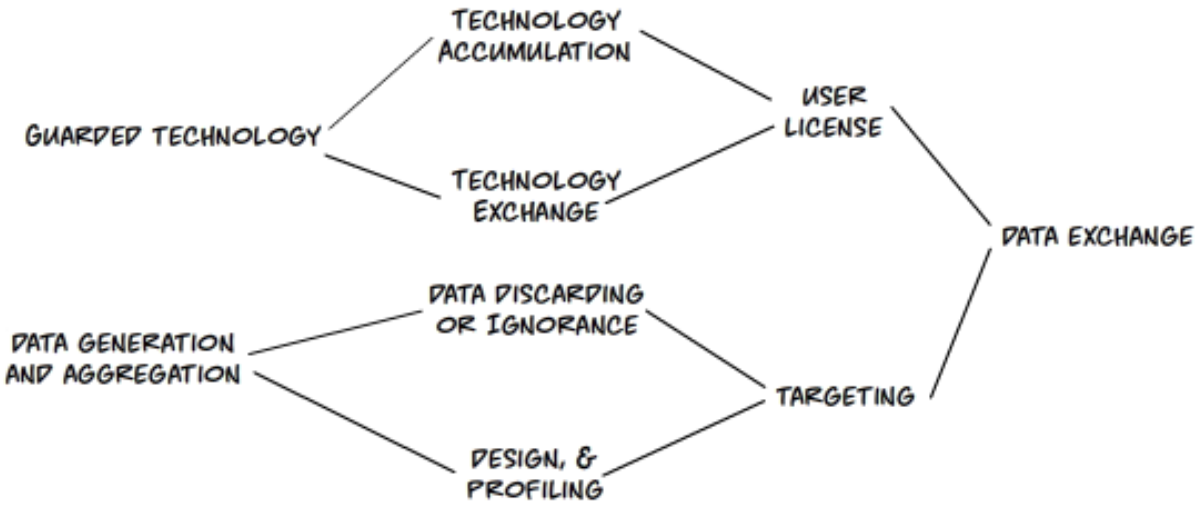

Figure 10 - Data Exchange

3.2.3.33 Third-Party API Data

Data generated from users' identity or data exchange can be used by APIs connecting tertiary and secondary operators. This data is used in the APIs to connect tertiary and secondary operators' apps and services with primary authentication processes. This allows users to perform authentication with third-party information systems. When using the OAuth process data channels about the user referred as flows move from party to another. Chapter 6 investigates the OAuth process closely.

3.2.3.34 Primary Authentication

User tokens used by people for authentication and third-party API data are involved in a recursive process that leads to primary authentication. Primary authentication is the initial authentication into an information system.

3.2.3.35 Advertisers

Advertisers are the third parties without platforms that rent space or time to reach audiences. Advertisers reach audiences through data exchanged from user licenses and platform operators' targeting. Advertisers use this data to track audiences across the platforms they advertise in. Sometimes, the tracking is performed through tools provided by platform operators. Sometimes advertisers develop their own trackers. There are two types of audience tracking performed by advertisers. They are opt-in tracking and opt-out tracking. Opt-in and opt-out tracking are not performed necessarily through authentication. These are practices that exist with digital media regardless of whether users are identified through a platform or not.

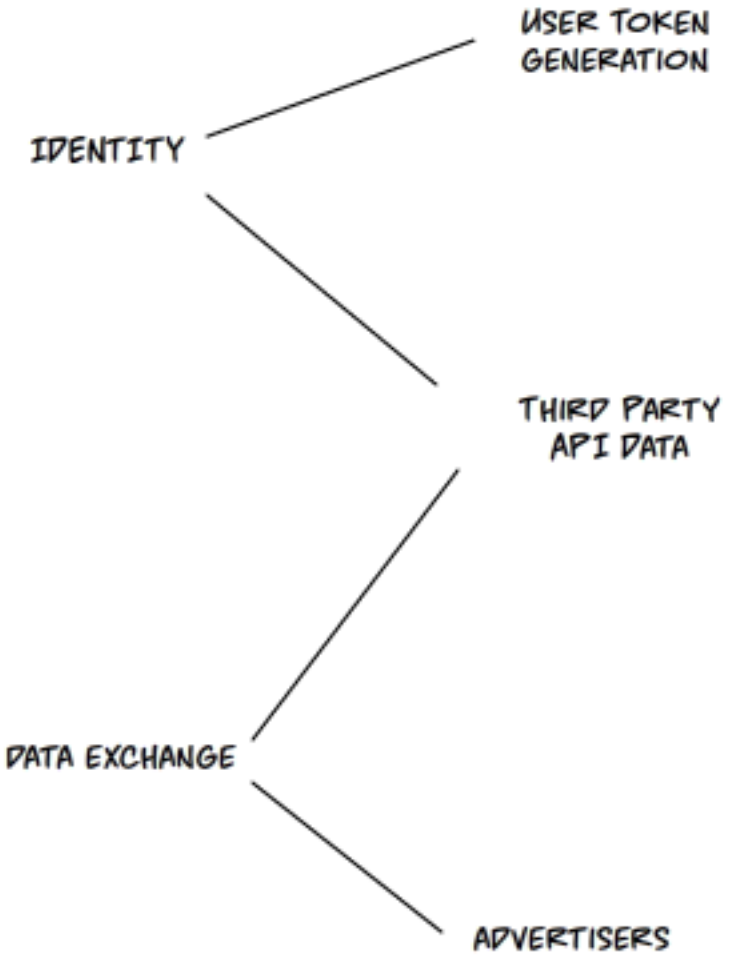

Figure 11 - Third Parties and Advertisers

3.2.3.36 Opt-In Tracking

Opt-in tracking is performed through database of users (audiences) generated or bought by advertisers with personally identifiable information.

3.2.3.37 Opt-Out Tracking

Opt-in tracking is performed through database of user (audiences) generated or bought by advertisers without personally identifiable information.

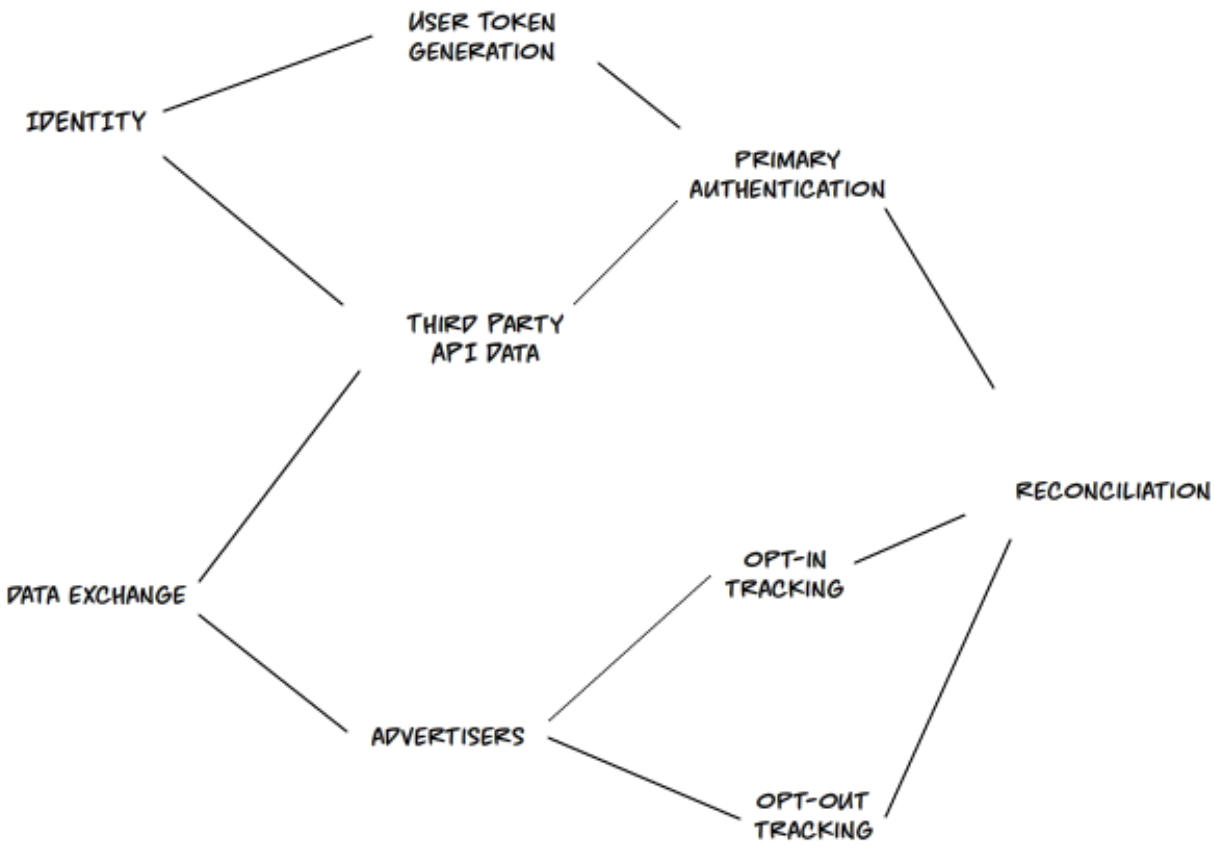

Figure 12 - Reconciliation

3.2.3.38 Reconciliation

Reconciliation is the compiling of several databases of user data stemming from monetization schemes and user registration. Reconciliation occurs from three sources; data obtained from primary authentication, opt-in tracking, and opt-out tracking. At the reconciliation stage, these data are integrated and complete the process of commodification that I described as the transactional token. Reconciliation is the culmination of the transactional token but also the starting point of this dialectic and recursive process where authentication and the monetization of attention split into two branches that merge and separate again, depending on the site of interaction with audiences.

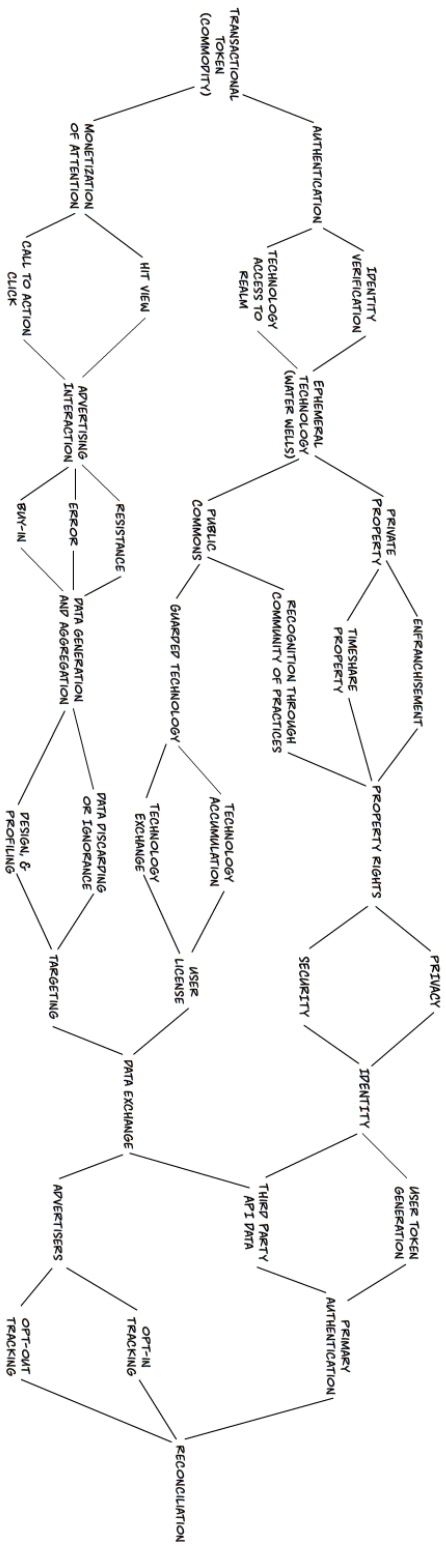

Figure 13 - Transactional Framework

3.3 Conclusion

The transactional token framework introduced in this chapter informs the design of the quasi-experiment and the policy analysis used in this study. This framework is a dialectic model that analyzes at once authentication and the monetization of attention while focusing on tertiary authentication. When applied as an analytical model, it can provide a significant critical understanding of processes that have been analyzed differently in the past. This framework is based on control point analysis, a method that can benefit HCI research because of its focus on step-by-step approach to interaction.

3.4 Research Conjectures

The transactional token theoretical framework proposed above offers a glimpse of the necessary evaluation of the users' perceptions of security and confidentiality as they perform tertiary authentications. To verify the study's claims, I rely on three conjectures which allow me to operationalize the research questions presented in the introduction chapter. Each conjecture tests one of the research questions empirically.

The first research question presented in the introduction seeks to determine is the extent of the interplay between security and usability for platform operators that are commodifying from users' personal data through tertiary authentication. The **RQ1** is answered partly in the policy analysis chapter (Chapter 6). In the Discussion (Chapter 7), the conclusions derived from the policy analysis are compared with the findings obtained from the first conjecture introduced below. These findings are presented in Chapter 5.

a) Conjecture 1 (C1) - I wanted to understand how closely or not user perceptions of security and confidentiality demonstrated through their tertiary authentication practices and mental models indicate an understanding of the authentication process developed by platform operators?
    a. How do users represent their mental models about tertiary authentication using diagrammatic elicitation?
    b. How do users' mental model differ from the design models of platform operators?

c. To test this conjecture, participants are asked to draw their mental models using pre-fabricated symbols representing nodes, sites, devices, platforms, and the network.

Based on my review of the literature and the elaboration of my theoretical framework, I am proposing two more conjectures to answer my second and third research questions through an quasi-experiment with participants. **RQ2** asks about how people manage and control their security and confidentiality as they perform tertiary authentications and what are the implications of those actions for users' perception of identity and privacy. **RQ3** asks about the factors and variables affect users' sense of security as they perform tertiary authentication. These conjectures seek to predict how people perceive and respond to tertiary authentication using a quasi-experiment and a survey.

b) Conjecture 2 (C2) - Finally, I was interested in how users manage and control their security as they perform tertiary authentication; how their practices could affect their perceptions of confidentiality and privacy related to the possible commodification of their interaction data by platforms and third?
    a. How do users process information about their privacy?
    b. How do users process information about their identity while performing authentications?
    c. To test this conjecture, participants are asked to adjust their account settings for each platform.
c) Conjecture 3 (C3) - When told that the personal information platforms share with third parties while performing a tertiary authentication is not editable or removable, will users will rate the security of their personal information as less secure and less confidential?
    a. How do users confer meaning to the exchange of information about their privacy?
    b. How do users confer meaning to the exchange of information about their identity?
    c. To test this conjecture, participants are asked to read the user agreement and privacy policy of each platform.

Conjecture 1 is related to Research Question 1. Conjecture 2 is related to Research Question 2. Conjecture 3 is related to Research Question 3. **Table 3** displays the mapping of each research question and conjecture.

Table 3 - Research Questions to Conjecture Mapping

Research Questions	*Conjectures*
RQ1	C1
RQ2	C2
RQ3	C3

In the next chapter, I present the research design used to delineate my inquiry into user perceptions of security and confidentiality while performing tertiary authentications and the commodification of their personal information by platform operators. I will justify the methods I used to yield persuasive results to support the research questions and conjectures of this dissertation. The methods I rely upon are qualitative and quantitative. Specifically, I rely on a policy analysis of platform operators' security and confidentiality policies, and a quasi-experiment and a survey of participants.

Chapter 4
Research Approach

In this chapter, I present the research method used to operationalize the three conjectures introduced at the end of Chapter 3. Conjecture 1 (C1) compares the divergence in practices and mental models of participants with the design models of Facebook, Google, and Twitter. This conjecture measures **RQ1**. Conjecture 3 (C3) measures how users rate the security of their personal information when aware that it is not editable or removable while performing tertiary authentication and shared with third-parties. Conjecture 2 (C2) measures user control and management of personal information during tertiary authentication. As seen in Table 3 in the previous chapter, Both **C2** operationalizes **RQ2**, and **C3** operationalizes **RQ3**. Here is a reminder of the dissertation's three research questions;

a) **RQ1** - What is the extent of the interplay between security and usability for platform operators that are commodifying from users' personal data through tertiary authentication?
b) **RQ2** - How are people managing and controlling their security and confidentiality as they perform tertiary authentications and what are the implications of those actions for users' perception of identity and privacy?
c) **RQ3** - Which conditions and variables create a perception of false security in users performing tertiary authentications, and what factors of tertiary authentication affect users' sense of security?

To answer these questions about user perceptions of tertiary authentication, I perform multiple evaluations. Methods include a policy analysis of the authentication practices of platform operators; a quasi-experiment assessing participants' use of authentication; and the administration of a survey of participants. Each evaluation corresponds to one of my research questions but also informs the overall study. The findings of the quasi-experiment are presented in Chapter 5. The results of the policy analysis are presented in Chapter 6.

4.1 Research Design

The study is undertaken through two sets of evaluations around the same sites. They are a policy analysis, and a user-based quasi-experiment which includes a questionnaire and diagrammatic representations of participants' mental models. The policy analysis allows an investigation into the trade-offs between security and usability from the perspective of platform operators. The policy analysis explores public documents from the platform operators. Although the analyses performed in this part of the study are based in part on social sciences research practice, I introduce an interaction lens to the analysis that is decidedly influenced by the human-computer interaction focus of this study.

The second set of evaluation methods are based on a quasi-experiment exploring how people manage and control their privacy and confidentiality. It explores the implications of tertiary authentications and people's sense of identity and privacy, as well as trying to identify factors that create in them perceptions of false security. The quasi-experiment includes a test and a control group of 20-participants (aged 18-68) who performed a series of primary, secondary, and tertiary authentications, and then related their experience in the form of diagrammatic representations of their mental models. Following the series of tasks performed by participants, they were invited to respond to a questionnaire and their responses were combined with the diagrammatic representations of their mental model to provide a broader understanding of people's security, and privacy practices, when performing tertiary authentications.

4.1.1 Policy Analysis

The first approach and methods for analyzing the policy analysis of data and privacy policies from Facebook, Google, and Twitter is framed by a perceptual evaluation that I introduced in the literature review chapter. This approach, inspired by similar work by Dourish (2001), frames the history of computer science through an interaction lens. Instead of the traditional way of perceiving computing developments as milestones or events, this approach favours looking at how people's interaction with technology changed and how that influence alters authentication.

Dourish labelled his approach to evaluating human-computer interaction **embodied interaction**. Embodied interaction evaluates people's interaction with computers that occupy our space and is part of our social reality (2001, 3). This approach is biased towards interaction rather than interface. Specific designs matter less than the activities we perform at sites of interaction (Dourish 2001, 3). Dourish favours understanding people's everyday activities instead of analyzing algorithms and procedures, which are behavioural and instrumental evaluations of information systems (2001, 3).

Embodied interaction is based on phenomenology and borrows heavily from ethnomethodology (Dourish 2001, 74). In this study, I have chosen to use the term perceptual approach to human-computer interaction rather than embodied interaction. Although strongly influenced by Dourish's work, by relying on the term 'perceptual' I focus less on themes such as ubiquitous mobile computing and more on how people acquire information from their interactions with information systems.

A perceptual approach focuses on user interactions with technology. The site of interaction where a person uses a technology is wrought with affordances about what he can or cannot do; how he can change a technology; and of course, how can a technology change him. My definition of affordance is inspired by Norman's. For Norman, affordances are how a person determines what can be done with a thing (2013, 11). The site of interaction is the place where a person interacts with a technology.

The second approach for performing the policy analysis relies on frame analysis to develop the coding of the documents. Frame analysis is a theoretical framework developed by Goffman (1974) attempting to find the meaning behind interactions be they natural or social based on a subject's own experience. According to Goffman, subjects, be they humans or animals create meaning about what they experience (1974). Frames have been compared to mental models as they depict the mental processes that determine how things work (H. Johnston 1995).

The mental model processes as frames approach has been prevalent in communications studies where frames are used to analyze how political actors and the media "frame" a story for

the public (D'Angelo and Kuypers 2010). Frame analysis has largely been forgotten and unused in other social sciences. Its use in communications and media studies is specific and defined as a rhetorical process (Kuypers 2009).

While aspects of the "framing of the story" are relevant for my policy analysis when determining the story behind how platform operators write policy documents, I seek to return to the interaction theories unearthed by earlier definitions of frame analysis. Frame analysis was perceived as a structuralist theory because it presupposed that frames in nature are structures that cannot be modified through human agency (Jameson 1976). Some frames, for example, like how people shake hands, are structural and not something that can be modified by individuals.

However, at the same time, this rigid definition of framing allows the individual, or a group to redefine the meaning of a structure. For example, Goffman explains play as keying, a form of framing where another type of interaction is copied but transformed into something else (1974). For keying to occur, both participants must accept to a new set of rules or a new frame.

It is this aspect of framing which is useful for the policy analysis. In a policy document, there is a structural contract that the platform operator provides to the end user, or the third-party developer about how to use the platform or its APIs. The platform operator also limits its own practices and responsibilities *vis-à-vis* the user or the developer. For example, 'This is how your personal data will be used should you agree to play this game with me.'

This document is presented to the user or the developer in a way that allows for them to carefully peruse through the first time they are faced with it, or to return to this contract after having agreed to it. Unlike the public, developers typically get stacks of documents that they can study carefully well-ahead of any commitment to the platform and without any pressure to agree to its contents.

I attempted to use the same versions of documents employed at the time of the quasi-experiment with participants (September-October 2016). I included a reading of additional documentation, when available. For example, Google has released a newer policy on March 1st, 2017. A comparison between the two versions revealed that Google replaced the term 'Google

Apps' with 'G Suite'. These are the only differences between Google's August 29, 2016 privacy policy and the March 1st, 2017 version.[10]

The third approach that I used for the policy analysis is based on the transactional token framework introduced in this study. This framework is itself in continuity with Dourish's perceptual approach by using social theory to explain the relationship between authentication and commodification. An important component of the transactional token framework is control point analysis and its focus on the site of interaction between a human and a technology.

Before advancing further in the policy analyses, I provide needed background information on the technical infrastructure upon which tertiary authentication is built.

4.1.2 User-Based Quasi-Experiment

I tested my research questions with a between-subject quasi-experiment collecting qualitative data about participant's representation of their mental models and their responses to a questionnaire. **C1** involved participant elicitation of mental models through diagrams after each experimental task. **C2** and **C3** required participants to respond to a questionnaire after the post-task. This study is a quasi-experiment mainly because participants were not randomly assigned to control or test groups (Cook and Campbell 1979).

4.1.2.1 Measures and Instruments

The study's larger independent variable is the authentication performed by participants. The broad dependent variable is participants' perceptions of security and confidentiality risks.

C1 is about the divergence between participants and platform operators' conceptual models of tertiary authentication. As a research question, this is not a classical hypothesis tested through an experiment. It is an observation of the results of participant's representation of their mental models about their perception of security and confidentiality when performing tertiary

[10] The policies used are not included in the Appendices but can easily be located on each platform operator's site.

authentication. The **comparison measure** is the design models of platform operators (Facebook, Google, and Twitter) about the tertiary authentication process. The **dependent measure** is the divergence and level of difference between of participants' mental models about tertiary authentication with platform operator's design models. The metrics used to test these divergence between conceptual models are the diagrammatic mental model representations of participants. I tested whether they adhered or not to the design models of primary platform operators.

The independent variable for **C2** is participants' explicit knowledge that the personal information shared by primary platforms with third-parties' apps are neither editable nor removable. The dependent variable for **C2** is participants' selective restriction of third party apps access to their profile.

The intervention used to test participants' security and confidentiality management, asked them to adjust their account settings for each platform. Only the test groups were asked to adjust their Facebook, Google, and Twitter settings. The metrics used to measure this research question are the results from the questionnaires answered by participants. I am interested in the results in **Q4**, **Q7**, **Q9**, **Q10**, and Q11 (**Table 4**) where I asked participants about their control over their personal data with regards to tertiary authentication.

Table 4 - Likert Scales

Q1 (C3) Any third-party app I log into from Facebook, Google, and Twitter is safe because it has been validated by each company before it was released to the public.
Q2 (C3). My experience using Facebook, Google, and Twitter with third party apps was as convenient, safe and confidential whether I used a laptop, tablet, or phone.
Q3 (C3). Using Facebook, Google, and Twitter to login into other apps is convenient.
Q4 (C2). I can edit or delete information from Facebook, Google, and Twitter used by any of these apps Angry Birds Friends, Business Organizer for Google Docs, dlvr.it, Dropbox, Google Docs, Instagram, Medium, Spark, Talon, or Vine.
Q5 (C3). I always read all of the terms of use and privacy policies of a new when installing and using a new platform or an app.
Q6 (C3). Do you ever go back to read terms of use and privacy policies after having used a platform or an app?
Q7 (C2). If you delete your Facebook, Google, and/or Twitter account do you trust that your information will be permanently deleted?

Q8 (C3). Using cloned clients such as Facebook for Blackberry Playbook, Sparks, and Talon, is as safe as using the original apps - Facebook, Google, and Twitter.
Q9 (C2). I adjust my security and confidentiality settings as soon as I install a new platform or an app.
Q10 (C2). I review and update security and confidentiality settings after having used a platform or app.
Q11 (C2). Do you verify that all your information has been deleted when revoking access to third-party apps like dlvr.it, Organizer for Google, Spark, Hootsuite, Facebook for Playbook, Talon, Dropbox, Angry Birds Friends, and/or Medium?

The **independent variable** for **C3** is participants' explicit knowledge of what personal information platform operators share during tertiary authentication processes. The dependent variable is participants' rating (evaluation) of the value of their security.

The intervention used to test participants' security and confidentiality awareness, asked them to read the user agreement and policy privacy of each platform. Only the test groups were asked to read the policies from Facebook, Google, and Twitter. The metrics used to measure this research question are the results from the 20-question questionnaires answered by participants after the experimental tasks. I am interested in the results in **Q1**, **Q2**, **Q3**, **Q5**, **Q6**, and **Q8** (**Table 4**) where I asked participants about the security and confidentiality of their personal information with regards to tertiary authentication.

4.1.2.2 Tasks and Procedures

The study involved users' Facebook, Google, and Twitter accounts. Participants adjusted accounts settings in a pre-task to allow the experiment to proceed, and to perform one initial a primary authentication. Primary authentications are authentications done within a single platform without exchanges between the user and a third party. Only the nine tasks comprising testing for the tertiary authentication were analyzed for this study

The post-task occurred after the task completion. I encouraged participants to return their settings to their original states. The post-task helped us monitor any changes in how participants managed their security and confidentiality. They were debriefed at the end of the entire experiment. I did not record screen-based data. I only used notes, questionnaire results, and diagram captures.

The pre-tasks and post-tasks were not pre-tests and post-tests. I did not compare variation in user data before the pre-task and after the post-task.

Table 5 - Experimental Road Map

Intervention 1	To test participants' security and confidentiality awareness, they were asked to read the user agreement and policy privacy of each platform.
Intervention 2	To test participants' security and confidentiality management, they were asked to adjust their account settings for each platform.
Type of Study	Quasi-Experiment
Measures & Instruments	Questionnaire administered post intervention after each task
Participants	20
Conjecture 1	Participants' diagrams
Conjecture 2	Q4, Q7, Q9, Q10, Q11
Conjecture 3	Q1, Q2, Q3, Q5, Q6, Q8

The study was a between-subject quasi-experiment where each participant completed every task before representing them on a drawing board. When done with their representations, investigators recorded the diagram drawn by participants who would then proceed to the next task. The order of the tasks was randomized for each participant. Participants had to perform 15 tasks. Three of the tasks tested primary authentication with Facebook, Google, and Twitter. Three secondary authentications with each primary platform were also tested. Finally, each of the three kinds of tertiary authentications (nine in all) were tested with each primary platform. Although I collected data on primary and secondary authentications, as mentioned above, these were not evaluated in this study. When the participants were done with the tasks, and the post-tasks, they responded to a 20-questions questionnaire described in **Table 4** and **Table 6**. Questions 1-11 used Likert Scales. Questions 12-20 were open-ended.

All apps and services used are benign and widely used consumer products. None supported illegal activities or tasks harmful to participants. These are the secondary apps used in tasks: Instagram (with Facebook), Google Docs (with Google), Vine (with Twitter). **Table 36** contains a full list of all tasks, platforms, and apps used.

4.1.2.3 Tertiary Data Manipulation Tasks

dlvr.it was used on a laptop computer. After performing a tertiary authentication through Facebook, participants had to add an RSS feed from a news blog to their new dlvr.it account to would send updates to their Facebook accounts.

Organizer for Google Docs was used on an Android tablet. After a performing tertiary authentication through Google, participants had to move a file from one Google Docs directory to another.

Hootsuite was used an iPad. After performing a tertiary authentication through Twitter, participants had to favorite the tweet of a person they follow on Twitter.

4.1.2.4 Tertiary Client Clone App

The Blackberry Facebook client was used on a Playbook tablet. After performing a tertiary authentication through Facebook, participants had to find and like a post from someone in their network. I chose the Playbook Facebook app because it is one of the few Facebook client still available.

Spark was used on an iPad. After performing a tertiary authentication through Google, participants had to send an email from their Gmail account through Spark to an address provided by the investigators.

Talon was used on an Android tablet. After performing a tertiary authentication through Twitter, participants had to post a tweet.

4.1.2.5 Unrelated Tertiary Service and Product

Each app in this section was tested on a laptop computer.

AngryBirds Friends accessed through the gaming area of Facebook. After performing a tertiary authentication through Facebook, participants had to install and play the first level of the game for about a minute of two.

Dropbox was accessed after performing a tertiary authentication through Google, participants had to accept to download Dropbox once their account had been set up.

Medium was accessed after performing a tertiary authentication through Twitter, participants had to pick story topics and follow one or two users.

After each task, participants had to logout or shut the application entirely. Investigators scrubbed each device used in the presence of participants during the debriefing period after the questionnaire were answered.

4.1.2.6 Diagrammatic Mental Model Representation

After each task, we invited participants to draw their mental models based on their perceptions of the interactions between the platforms and the apps. They received no instructions about how to represent their mental models, thus controlling for any confounding variables. The diagrams created by the participants were coded and recorded as photographs, so they could be analyzed.

I used a set of magnetic icons (**Figure 14**) representing every platform and app used in the study allowing participants to create links, draw relationships, or add ideas. As well as using the magnets, participants were provided multiple markers that they could use on the white drawing board with the magnets. This process resembles coding possible answers in a Likert scale questionnaire. Without the pre-fabricated icons, used as coded building blocks, it is likely that the mental models participants represented would have be vague and of little use for the study. Each number in the blue circle indicates the total number of icons generated per concept represented.

Figure 14 - Magnetic Icon Chart

Here is an example of the instructions participants received from investigators after each task. Except for the specific task mentioned, the instructions used the same format.

Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings your interaction with the device, the software, and the website. Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

4.1.2.7 Questionnaire Data

Participants answered the questionnaire after completing the experiment. I evaluated their security and confidentiality practices when performing different authentications. The questions sought to correlate participant's practices with the interventions tested in the experiment.

The second section of the questionnaire asked broad open-ended questions about the study in general. I used the responses as qualitative insights about the overall study and did not test them against specific research questions. Q12-to-Q20 (**Table 6**).

Table 6 - Open-Ended Questions

Q12. Did you notice any differences between the different ways that you logged into each platform and app? Explain in your own words.
Q13. Did you experience any difficulty while logging into the different platforms and apps? Explain in your own words.
Q14. How did you feel about logging into Facebook, Google, and Twitter to perform tasks? Did you have any concerns about the security of your information?
Q15. What security measures would you take to secure yourself when you log in to Facebook, Google, and/or Twitter?
Q16. What are some of the tips that you would give an acquaintance to remain secure when using Facebook, Google, and/or Twitter?
Q17. Do you feel that your information is safer because Instagram, Google Docs, and Vine are owned respectively by Facebook, Google, and Twitter?
Q18. What happens to your information from Instagram, Google Docs, and Vine if you delete your Facebook, Google, and, or Twitter accounts?
Q19. If you delete your Facebook, Google, and/or Twitter account, what should happen with the information collected independently by dlvr.it, Organizer for Google, Spark, Hootsuite, Facebook for Blackberry Playbook, Talon, Dropbox, Angry Birds Friends, and/or Medium?
Q20. In your words, what are security and confidentiality? Are they the same? What about privacy?

4.1.2.8 Test and Control Groups

Twenty participants were enrolled in the quasi-experiment. A Latin square was used for randomization, with four distinct groups of five participants each. Test groups were exposed to either the first or the second intervention (Yes/No or No/Yes), both interventions (Yes/Yes), or

neither (No/No). The control groups for the first intervention are No/No and No/Yes. The control groups for the second intervention are No/No and Yes/No.

4.1.2.9 Participants

I recruited 20 adult participants located in the Toronto area, a large predominantly English-speaking metropolitan area in Canada. Ten men and ten women took part in the quasi-experiment which did not control for other demographic metric such as age, education, or level of technological literacy. Participants had accounts with the primary platforms. I attempted to filter out candidates who had used the tertiary apps previously but a few failed to disclose their prior usage. Some forgot that they had created accounts with some apps previously. The results of the participants are generalized to the population that uses the Internet, specifically social media and the main platforms selected (Facebook, Google, Twitter) as the site of the study.

4.1.2.9.1 Recruitment of Participants

Figure 46, in the Appendices, contains a copy of the recruitment poster. Sessions with participants lasted between two and a half-hour to three hours and were held at specific dates and days of the week.

The recruitment controlled for age, computing and social networking literacy. Investigators tested participants' literacy by asking them about their usage level of Facebook, Google, and Twitter. The only recruitment data retained and used for analysis during the study are participants' age group and gender.

I used an email-based self-evaluation survey to perform some stratification and clustering before allowing applicants to enter the pool of potential randomly selected participants. Stratification ensures the equal representation of women and men in the quasi-experiment.

Candidates that answered positively about their usage of the three platforms within the last three months, and who had working accounts were eligible to join the pool of potential participants. **Table 37** in the Appendices contains a copy of the self-screening survey.

Clustering sampling guaranteed that participants have basic mobile computing and social networking literacy. I sought to represent adult males and females from the Toronto area population with mobile and social network computing. As indicated in the recruitment ad, the social networking literacy of participants is determined by asking them if they had a social network account from Dropbox, Facebook, Google, LinkedIn, or Twitter in the last three-months. The literacy required of participants for mobile computing literacy is having used Facebook, Google, or Twitter with a smartphone, or a tablet for the last three-months. I also asked applicants about their gender, if they are adults, and if they live in the greater Toronto area and can travel to the test site at the St. George campus of the University of Toronto. Applicants who did not fulfill these basic literacy skills, age range, and location criteria were not invited to become potential participants. **Table 38** in the Appendices contains demographic information about the 20 participants. Scenario refers to the two conditions participants were tested for. This is covered further below.

Participants agree to use their personal accounts for the study. Study investigators[11] did not retain any data stemming from the participants' accounts and the new ones that they create during the quasi-experiment. Investigators did not directly monitor or browse through participants' accounts. I was interested in how they interacted with tertiary apps and primary platforms.

4.1.2.9.2 Informed Consent

Informed consent was obtained through a form stating how the data would be used. Participants signed the form prior to the start of the quasi-experiment and the pilot. A copy of the Informed Consent Form is available in **Figure 47** and **Figure 48** of the Appendices.

[11] The study's investigators included myself, and two assistants. One was a master's student and the other was an undergraduate. Both attend the University of Toronto.

4.1.2.9.3 Participants Confidentiality and Data Retention

Participants IDs were used instead of their names for research materials. However, a separate list with their names was retained as well as signed receipt for the gift cards to keep records for financial audits.

Participants were assigned a participant number pairing all data collected about them with this identification. A master list containing participant names and numbers was maintained during the data collection process.

The master list containing participant names was kept in a locked cabinet in a secure room at Semaphore Lab at the Faculty of Information until data collection was completed. All anonymized data is stored electronically on password protected hard drives, until the analysis is completed or a maximum of 36 months.

Consent forms and receipts used for financial audits are kept apart from other research material in a different locked cabinet at the Faculty of Information.

The data will be treated in confidentiality according to all relevant provincial (Ontario) and federal (Canada) legislation.

4.1.2.10 Data Analysis

I chose to perform nonparametric analyses of the closed-ended questions (the Likert Scales) with a Mann-Whitney U test. I considered two other nonparametric procedures (median tests, and Kruskal-Wallis tests) but the Mann-Whitney U test is ideal for ordinal data with only two independent samples (Mackenzie 2013, 215).

To analyze the open-ended answers one investigator and a doctoral student assisting with the research did independent first-pass qualitative coding evaluations. The investigator coded mainly for patterns to obtain as much insight from the data collected. The doctoral student coded with the questions from the questionnaire in mind, attempting to limit the categories. The results from this first-pass coding sometimes matched and often did not. We discussed the divergences and tried to resolve our differences and find common themes. From the collected first-pass

coding evaluation, we performed a second-pass coding to find codes adhering to **C2** and **C3**. Thus, we limited categories so that they could be analyzed with descriptive statistics.

We analyzed the diagrams qualitatively. First, we wrote qualitative reviews of each diagram to begin developing terms and a language about the dataset. We remained open-minded and relied on a grounded theory approach (Corbin and Strauss 1990) to record observed patterns. After our initial annotations, we observed six themes (**Table 7**) that could be transformed into questions about the participants' diagrams.

Table 7 – Six Qualitative Themes

Is there a login?
Is there a log out?
Which devices were used in the tasks?
Which steps were covered or not?
Relationships between primary, secondary and tertiary indicated?
Reaction to access rights requested?

I wrote qualitative summaries of each diagram based on the six questions. These six questions allowed us to observe more patterns in the representation of authentication by participants. Using the six questions as our core, I was able to refine them into 14 detailed questions/themes (**Table 8**) which were then used to perform more analysis.

Table 8 - List of Questions Drawn from Themes

Is there a login?
Is there a log out (PC) or exit from app (mobile)?
Are there modalities of interactions?
Are the modalities in the interaction path?
Relationships between primary, secondary and tertiary indicated?
Reaction to access rights requested?
Is it a linear interaction path?
Abstract or physical Model?
Are there pairs as sites of interaction?
Does the primary platform precede the tertiary authentication?
Is the tertiary authentication part of the interaction path?
Differentiation of the operating system from the device (mobile), the browser from the PC (PC), or Indication of independent Internet (both).

What or where is the initial site of interaction?

What is the last site of interaction?

The user-based quasi-experiment involved 20 participants. The quasi-experiment tested two conditions. The first condition measures participants' perceptions of security and confidentiality with tertiary authentication. The second condition measured participants' control and management of security and confidentiality with tertiary authentication. The quasi-experiment included a pre-task, five tasks that participants had to perform and a post-task for each of the three platforms evaluated (Facebook, Google, and Twitter). The quasi-experiment was designed as a between-subject study. The order in which participants tested each platform was randomized. **Table 36** in the Appendices contains a full list of all tasks performed by participants.

Participants in the pilot and the quasi-experiment performed various tasks on devices provided by the investigator. They used a desktop, an Android tablet, an iPad, and a BlackBerry Playbook tablet. After each session with participants, their private data such as browser cookies, cache, and any other private elements, were erased. Participants use devices that have been scrubbed of any previous private data. **Table 35** (in the Appendices) contains a copy of the quasi-experiment's protocols.

4.1.2.11 Experimental Limits

The interventions used in the study relied on benign deception to gather data on participants' perceptions. In recruitment materials and conversations, participants were informed that they were participating in a mobile and social media literacy study. We wanted to control for any behavior related to handling their security, confidentiality, and privacy with the information systems used. Participants were properly debriefed and told about the real objective of the study after they completed all tasks, and the questionnaire. By reading and signing the consent forms that addressed the privacy and confidentiality usage of the data collected in the quasi-experiment before sessions began, participants may have been exposed to unavoidable confounding variables. IRBs were obtained from the university's research ethics office.

We did not monitor participants' screens nor record any data related to their personal social media accounts. No measurement of changes in their settings were recorded formally throughout the study to adhere to IRBs regulations. This explains why our study relied on pre-tasks and post-tasks, instead of pre-tests and post-tests. Only when providing support with devices and apps to participants who requested it did the study's investigators have access to participants' personal information displayed on screens.

The study focused on user perceptions, not on the effects of platform operators' usage of people's interaction data as they performed tertiary authentication. We could not obtain official design models for each task. The range of apps and services and devices was too broad to permit us to have official documentation from Facebook, Google, or Twitter. Instead, we recreated potential design models and read them to participants. Investigators and research assistants performed many of these tasks ahead of time, recorded each step and evaluated them before transcribing them as instructions we could read to participants.

4.2 Conclusion

The next chapters will present the findings of the quasi-experiment and of the policy analysis. Chapter 5 will present the results of the quasi-experiment with the participants. They performed 15 tasks followed by diagrammatic representations of their mental models. Each participant then answered a questionnaire. The data from the quasi-experiment contrasts with the one from the policy analysis in Chapter 6 which explores how platform operators Facebook, Google, and Twitter enable tertiary authentication. The policy analysis is framed within transactional theoretical framework introduced in Chapter 3. Chapter 7 discusses the results from Chapter 5 and 6 and provides responses to the three research questions of this dissertation.

Chapter 5
Findings – Experimental Results

In this chapter, I present the results of the quasi-experiment conducted with 20 participants where I tested three conjectures about users' perception of security and confidentiality risks as they perform tertiary authentications. Conjecture 1 helps me answer Research Question 1 along with the findings from policy analysis presented in Chapter 6. **RQ1** asks to what extent of the interplay between security and usability for platform operators that are commodifying from users' personal data through tertiary authentication. Conjecture 2 helps me answer **RQ2** which asks how people are performing tertiary authentications as they manage and control their security and confidentiality and about the implications of those actions for users' perception of identity and privacy. It investigates the implications of those actions for users' perception of identity and privacy. Conjecture 3 helps me **RQ3** which asks about the conditions and variables that create a perception of false security in users performing tertiary authentications. It looks at the factors of tertiary authentication creating a false sense of sense of security with users.

Conjecture 1 involved participant elicitation of mental models through diagrams after each experimental task. Conjectures 2 and 3 required participants to respond to a questionnaire in a post-task following the experimental tasks that I asked them to complete.

a) Conjecture 1 compares the divergence in practices and mental models of participants with the design models of Facebook, Google, and Twitter.
b) Conjecture 2 measures user control and management of personal information during tertiary authentication.
c) Conjecture 3 measures how users rate the security of their personal information when aware that it is not editable or removable while performing tertiary authentication and shared with third-parties.

In the first part of this chapter, I review the findings from Conjecture 1 which involved diagrammatic-elicitation from the 20 participants. In doing so, I briefly cover the theoretical background related to the diagrammatic-elicitation pioneered in this study. In the second part of this chapter, I review the questionnaire findings from the quasi-experiment. These questionnaire

findings are supplemented by ethnographic notes taken about the participants as they performed the quasi-experiment.

5.1 Questionnaire Results

We report here on the qualitative and descriptive statistics of data collected through the post-task questionnaire. The Mann-Whitney tests did not reveal any statistical significance for **C2** and **C3** with respect to the differences introduced by the tasks and by the knowledge gained by participants, likely due to the strong effects personal differences had over a very short-term intervention. However, we discuss qualitative and descriptive results as to provide further insights that complement the rich data collected under **C1**.

C2 related questions tested if participants informed that their personal information was shared during tertiary authentication, restricted access to their profiles during the pre-task, the quasi-experiment, and the post-task.

C3 related questions tested how participants who had read the privacy and security policies from Facebook, Google, and Twitter rated the security of their personal information when aware that it is not editable or removable while performing tertiary authentication and shared with third-parties.

Table 9 - Closed Questions

Q1 (C3) Any third-party app I log into from Facebook, Google, and Twitter is safe because it has been validated by each company before it was released to the public.
Q2 (C3) My experience using Facebook, Google, and Twitter with third party apps was as convenient, safe and confidential whether I used a laptop computer, a tablet, or a smartphone.
Q3 (C3) Using Facebook, Google, and Twitter to login into other apps is convenient.
Q4 (C2) I can edit or delete information from Facebook, Google, and Twitter used by any of these apps Angry Birds Friends, Business Organizer for Google Docs, dlvr.it, Dropbox, Google Docs, Instagram, Medium, Spark, Talon, or Vine.
Q5 (C3) I always read all of the terms of use and privacy policies when installing and using a new platform or an app.
Q6 (C3) Do you ever go back to read terms of use and privacy policies after having used a platform or an app?
Q7 (C2) If you delete your Facebook, Google, and/or Twitter account do you trust that your information will be permanently deleted?

Q8 (C3) Using cloned clients such as Facebook for Blackberry Playbook, Sparks, and Talon, is as safe as using the original apps - Facebook, Google, and Twitter.

Q9 (C2) I adjust my security and confidentiality settings as soon as I install a new platform or an app.

Q10 (C2) I review and update my security and confidentiality settings after having used a platform or an app.

Q11(C2) Do you verify that all your information has been deleted when revoking access to a third-party apps like dlvr.it, Organizer for Google, Spark, Hootsuite, Facebook for Blackberry Playbook, Talon, Dropbox, Angry Birds Friends, and/or Medium?

5.1.1 C2 Questionnaire Results

The intervention which inquired about the participants' security and confidentiality management was measured by an independent variable with a condition asking them to adjust their account settings for Facebook, Google and Twitter. The post-task questionnaire then tested participants' security and confidentiality management. Questions 4, 7, 9, 10 and 11 tested participants' security and confidentiality management. Conjecture 3 proved null in every question observed. Encouraging participants to adjust their Facebook, Google, and Twitter privacy and security settings before performing the tasks did not create a condition that would influence participants' questionnaire answers. There were no subgroups or patterns that could be observed from the test and control groups. However, alternative conjectures testing provided an interesting observation, as will be covered below.

Table 10 - Question 4

4- I can edit or delete information from Facebook, Google, and Twitter used by any of these apps AngryBirds Friends, Business Organizer for Google Docs, dlvr.it, Dropbox, Google Docs, Instagram, Medium, Spark, Talon, or Vine.				
[Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree]

With **Q4**, 75% agree that they can edit or delete info used tertiary and secondary apps. A majority feels that they have control over their data once it has been exchanged with a tertiary app. 10% feel neutral, 15% disagree. It is interesting to note that although 75% of participants feel that they can edit or delete personal data from a primary platform held by a tertiary app, participants' perceptions may not match the actual technological affordance offered to them by Facebook, Google, and Twitter. Some of this data may not be editable or easy to delete. **Table 46** and **Figure 41** in the Appendices list the complete results and Mann-Whitney U test.

Table 11 - Question 7

7- If you delete your Facebook, Google, and/or Twitter account do you trust that your information will be permanently deleted?				
[Never	Rarely	Sometimes	Often	Always]

Looking at **Q7**, 55% of participants rarely or never trust that their information will be deleted. A strong 30% do not know or feel neutral about the statement. Only 15% trust that their information will be often or always deleted from the primary apps. These results contrast with those of **Q4** where participants felt more positive about being able to delete or edit their information if they were making changes directly with the tertiary apps. This question's results demonstrate a certain malaise with how participants perceived the usage of their personal information even when they actively sought its destruction. **Table 47** and **Figure 42** in the Appendices list the complete results and Mann-Whitney U test.

Table 12 - Question 9

9-I adjust my security and confidentiality settings as soon as I install a new platform or an app.				
[Never	Rarely	Sometimes	Often	Always]

Q9 measures how soon do users adjust their security and confidentiality settings. The results are not exactly consistent with those for **Q10**. Fifty-percent of participants claim to often or always adjust their security and confidentiality as soon as they install a platform or an app. However, results for participants who sometimes review or update their settings as they install a platform, or an app is closely related at 45%. This matches the 40% from **Q10** who sometimes adjust their settings. Participants seem to prefer adjusting their privacy and security settings than reading privacy policies and usage terms. **Table 48** and **Figure 43** in the Appendices list the complete results and Mann-Whitney U test.

Table 13 - Question 10

10-I review and update my security and confidentiality settings after having used a platform or an app.				
[Never	Rarely	Sometimes	Often	Always]

In **Q10**, 40% of participants (8) state that they sometimes review and update their security and confidentiality settings after having used a platform or an app. Twenty-five-percent of participants (5) often follow this practice. Ten-percent of participants (2) always do. Fifteen-percent of participants (3) rarely do. Ten-percent of participants (2) never adjust their settings. As conveyed in the Policy Analysis Chapter, there could be some form of platform-based

gamification effect that creates conditions where participants prefer interacting with privacy and security settings rather than reading about them. **Table 49** and **Figure 44** in the Appendices list the complete results and Mann-Whitney U test.

Table 14 - Question 11

11- Do you verify that all your information has been deleted when revoking access to a third-party apps like dlvr.it, Organizer for Google, Spark, Hootsuite, Facebook for BlackBerry Playbook, Talon, Dropbox, AngryBirds Friends, and/or Medium?				
[Never	Rarely	Sometimes	Often	Always]

As for **Q11**, 45% rarely or never verify that their information has been deleted when revoking access to a tertiary app. Thirty-percent of participants claimed that they did so. Twenty-five percent of participants claimed that they always or often verified that their information had been deleted after removing a tertiary app. The strong results for participants who claimed to verify their deleted information sometimes, often, or always is problematic as this is highly difficult to perform such a verification when an account is deleted. Even if such information was available, it would still be masked by the platform. It says much about their beliefs that they do control their personal information. This belief in their personal agency does conflict with the pessimism that many report as not being in control of their personal information. It highlights a classic agency versus structure debate noted by scholars such as Giddens (1984) and Beck (1992; 2000). **Table 50** and **Figure 45** in the Appendices list the complete results and Mann-Whitney U test.

5.1.2 C3 Questionnaire Results

The intervention which inquired about the participants' security and confidentiality awareness was introduced by asking them to read the privacy and security policies of Facebook, Google and Twitter. The post-task questionnaire then tested participants' security and confidentiality awareness. Questions 1, 2, 3, 5, 6, and 8 tested participants' security and confidentiality awareness. Conjecture 2 proved null in every question observed. Reading the privacy policies and terms of use of Facebook, Google, and Twitter did not create a condition that would influence participants' questionnaire answers. There were no subgroups or patterns that could be observed from the test and control groups.

Table 15 - Question 1

1- Any third-party app I log into from Facebook, Google, and Twitter is safe because it has been validated by each company before it was released to the public.				
[Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree]

Forty-five-percent of participants who answered **Q1** disagree that tertiary apps are safe even when validated by primary platforms. Thirty-percent are neutral and therefore unsure about how much protection is afforded to them by platforms. Only 25% agree. There is a sense of cynicism about tertiary authentication that makes participants pause before proceeding with the process. **Table 40** and **Figure 35** in the Appendices list the complete results and Mann-Whitney U test.

Table 16 - Question 2

2-My experience using Facebook, Google, and Twitter with third party apps was as convenient, safe and confidential whether I used a laptop computer, a tablet, or a smartphone.				
[Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree]

In **Q2**, 55% found their experience convenient, safe, and confidential whether they used a laptop, a tablet or a smartphone. Thirty-percent feel neutral about this. Fifteen-percent disagree. This question challenges the cynicism of the previous question. It is the same question as the first but with the addition of the term convenience. A possible answer for this is the addition of the usability and user experience dimensions with security and confidentiality. **Table 41** and **Figure 36** in the Appendices list the complete results and Mann-Whitney U test.

Table 17 - Question 3

3-Using Facebook, Google, and Twitter to log into other apps is convenient.				
[Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree]

When looking at **Q3**, 80% of participants feel that using tertiary authentication via Facebook, Google, and Twitter is convenient. This question reinforces the apparent contradiction found between **Q1** and **Q2**. This time, it is **Q2** but without the security and confidentiality aspects. The results are stronger in support of convenience, thus usability and user experience when security and confidentiality are no longer measured concerns. **Table 42** and **Figure 37** in the Appendices list the complete results and Mann-Whitney U test.

Table 18 - Question 5

5-I always read all of the terms of use and privacy policies of a new when installing and using a new platform or an app.				
[Never	Rarely	Sometimes	Often	Always]

With **Q5**, 60% rarely or never read privacy policies when installing a new platform or app. Is unclear how much of the 15% who claims to sometimes read privacy policies responded out of guilt or shame at what they feel they should be doing instead of what they do. It is unclear how systematic are the 25% who claim to read policies (i.e. do they only quickly glance?) Only 5% of participants claimed to always read the privacy policies. They are probably the most reliable in terms of their practices. Most participants indicated that they did not always read the terms of uses and privacy policies of new platforms and apps. Security is not a priority in the tasks they perform and their objectives. **Table 43** and **Figure 38** in the Appendices list the complete results and Mann-Whitney U test.

Table 19 - Question 6

6- Do you ever go back to read terms of use and privacy policies after having used a platform or an app?				
[Never	Rarely	Sometimes	Often	Always]

In **Q6**, 80% of participants rarely or never go back to read the terms of use or a privacy policy. Fifteen-percent sometimes do. Five-percent of participants do. As well as not reading the terms of uses or privacy policies when they first install new platform or apps, most participants never read such documents subsequently. It appears that policy documents are not favored by the sample in the study. Although a generalization to all Facebook, Google, and Twitter users is not statistically sound or valid, the sample probably echoes the practices of the population of these platforms. This would be something that platform operators have already measured and would understand how to best inform their users by promoting control panels that adjust security and privacy settings where users' interaction may be more significant.

This idea is supported in the sample with **Q10** where 40% of participants often or always review and update their security and confidentiality settings after using a platform or an app. Forty percent review and update their setting sometimes. **Table 44** and **Figure 39** in the Appendices list the complete results and Mann-Whitney U test.

Table 20 - Question 8

8- Using cloned clients such as Facebook for BlackBerry Playbook, Spark, and Talon, is as safe as using the original apps - Facebook, Google, and Twitter.				
[Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree]

The high level of neutral responses (50%) in **Q8** may indicate that participants were unaware of using clone clients in the case of the Playbook or that they never questioned the security of such apps in the case of Spark and Talon.

Yet 35% disagree or strongly disagree with the statement that using cloned clients is as safe as using the original primary platforms. It is unclear with the sample if the use of client apps was significant prior the experiment. It does not appear that many participants perceived the Facebook app for the BlackBerry Playbook as a third-party app. It appeared to be produced and distributed by Facebook. **P12** who denied access to many of the tertiary and secondary apps she was instructed to install (based on our notes and her diagrams) did not deny the Playbook Facebook app access to her Facebook account.

However, she did deny access to Spark while allowing Talon to access her tweets. The Spark task appeared earlier than the Playbook and the Talon tasks. Spark requested access to her email account. It appears that she valued her email through Gmail strongly. Her Facebook being semi-private and difficult to differentiate as a tertiary app would have been rated moderately while she granted access to a third party. Meanwhile, her tweets which she may not value as strongly were not blocked from Talon. Moreover, **P12** also did not block Hootsuite's access to her Twitter account. **Table 45** and **Figure 40** in the Appendices list the complete results and Mann-Whitney U test.

5.2 Qualitative Questionnaire Analysis

As mentioned above, the results for the qualitative part of the questionnaire were coded twice so that basic descriptive statistics analysis. We limited our reporting to questions pertaining to tertiary authentication (Q12, Q13, Q14, and Q19).

For **Q12**, 13 participants (65%) noticed a difference between the way they logged into each platform. For example, **P18** wrote "*Yes some apps will error (sic) and be unable to log me into the 3rd apps.*"

Some of the inconveniences that participants felt when performing tertiary authentications was related to problems encountered while performing the quasi-experiment, as expressed in answers for **Q13**. For example, **P05** and **P08** wrote that they encountered some problems because they forgot some of their passwords. **P13** had a similar experience and added "*Keeping track of the various user names & passwords as I went back & forth was confusing. Specifically, I confused my Twitter account username with that of another I use occasionally.*" **P16** and **P17** experienced problems with the Facebook app on BlackBerry who would crash frequently.

Other inconveniences appear less related to the quasi-experiment and more typical of what users may encounter every day: "*I had 2-step authentication that was causing difficulties, especially with Google on receiving code on the phone.*" (P09), or "*Hootsuite had some conflict between Twitter and Google and wouldn't work*" (P19, responding to Q13).

Answering **Q14**, **P05** wrote "*I had concerns because I thought the apps were going to post things without my consent [.]*" **P10** commented the concerns about the security of her information "*It was certainly convenient. I felt a niggling thought that maybe I should be worried about security but then dismissed it."* Participants may feel uncomfortable with tertiary authentication yet continue the practice. **P12** confirms this by writing "*I continue to use them as I see fit.*"

In **Q19**, 13 participants (65%) thought that personal information collected by tertiary apps and services should be deleted if they delete their Facebook, Google, or Twitter accounts. Five participants (5%) thought that the information was kept. While **Q4** and **Q11** asked related questions about personal data deletion, **Q19** tested how participants wanted tertiary apps to handle their data. Participants' responses were not just focused on what policy they wanted the platform operators to pursue but also on the difficulty of verifying that the information was deleted. This contrasts with **Q4** and **Q11** where participants felt that they had agency over their

personal information. This question appears to have made many participants recognize the impasse. **P15** wrote "*They can't access platform login so platform info is gone but app info could still exist… but how can we login now to delete it if account is gone?*" From participants' responses, there is a sense that that 'someone' other than them should take care of personal data left behind automatically. This is a genuine request for greater convenience and usability to be embedded in platforms and tertiary apps for the benefit of user experience. **P11** response to the question was "*INSTANTLY "DISAPPEAR.*" **P13** asked for a minimum of user convenience when she wrote "*You should at least be asked if you want it deleted or be given an option to create a new identity.*"

The participants answered a 20-question questionnaire that was handed to them during the post-task of the quasi-experiment. The questions were about their practices and perceptions of security, privacy, and confidentiality as they perform tertiary authentications. Eleven of the questions were closed-ended and relied on Likert scales. The remainder were open-ended. Some of the questions pertained to conjecture #2, some #3. The questions did not follow a sequential order. The answers from questions 1 to 11 are Likert scales which are analyzed as between-subject ordinal data to test conjectures 2 and 3 using nonparametric procedures in SPSS 24.0. Nonparametric procedures were ideal for a study with a small sample size.

5.2.1 Open-Ended Questions Coding

The open-ended questions in the questionnaire were not specifically crafted to answer **C2** and **C3**. To convert the open-ended answers collected in the questionnaire into a format suitable for conjecture testing, a doctoral student and I each performed one first-pass coding. In my coding, I coded mainly for patterns to obtain as much insight from the data collected. The doctoral student coded mainly with the questions from the questionnaire in mind and at hand, attempting to limit the categories. The results from this first-pass coding sometimes matched and often did not. We discussed the divergences and tried to resolve our differences and find common themes.

With the collected first-passes, I did a second-pass coding this time specifically focused on creating codes that adhered to conjectures 2 and 3. This meant that categories had to be

limited so they could be tested in an experimental context and used a data that was like the Likert scale answers from Questions 1 to 11. Below is a list of open-ended questions (12 to 20).

12. Did you notice any differences between the different ways that you logged into each platform and app? Explain in your own words.
13. Did you experience any difficulty while logging into the different platforms and apps? Explain in your own words.
14. How did you feel about logging into Facebook, Google, and Twitter to perform tasks? Did you have any concerns about the security of your information?
15. What security measures would you take to secure yourself when you log in to Facebook, Google, and/or Twitter?
16. What are some of the tips that you would give an acquaintance to remain secure when using Facebook, Google, and/or Twitter?
17. Do you feel that your information is safer because Instagram, Google Docs, and Vine are owned respectively by Facebook, Google, and Twitter?
18. What happens to your information from Instagram, Google Docs, and Vine if you delete your Facebook, Google, and, or Twitter accounts?
19. If you delete your Facebook, Google, and/or Twitter account, what should happen with the information collected independently by dlvr.it, Organizer for Google, Spark, Hootsuite, Facebook for Blackberry Playbook, Talon, Dropbox, Angry Birds Friends, and/or Medium?
20. In your words, what are security and confidentiality? Are they the same? What about privacy?

5.2.1.1 First Pass Coding

For the qualitative coding, I and a doctoral student[12] performed first pass analyses on questions 12 to 20 which were open-ended. I did not provide any instructions to the second coder so that we could compare and discuss similarities and differences once we each completed the first pass coding. When I performed the coding, I did not code with the questions or the conjectures in mind. I coded for patterns. The second coder coded with the questionnaire's questions in mind and attempted to limit categories. **Table 72**, in the Appendices, contains the full first pass qualitative coding.

[12] The second coder is Coder #4 described above in the Diagrammatic Representation Coding.

5.2.1.2 Second Pass Coding

Based on the first pass qualitative coding performed by a doctoral student and myself, I regrouped all categories under a simplified coding schema. I reused many existing open-ended patterns abandoned before the second pass to review data that would not fit the conjecture testing. **Table 73** includes the results. The second pass coding focused on the parts of the questions that could be answered with a yes or no. **Q15** and **Q16** had nominal data as responses. For these questions, participants could have multiple answers. I classified participants with multiple answers per participants into distinct classes. Below is a summary of highlights from each question.

Q12: thirteen participants (65%) noticed a difference between the way they logged into each platform. For example, **P18** wrote "*Yes some apps will error (sic) and be unable to log me into the 3rd apps.*" During the quasi-experiment, we noted that **P18** had problems using Dropbox with her Google account, got several errors when attempting to load the AngryBirds Friend app on Facebook, and problems using Twitter due to a Twitter outage that affected Eastern North America on October 21, 2016.

Q13: twelve participants (60%) had trouble when logging into different platforms and apps. The response to this question appears to contradict the one provided for **Q3** where participants were asked about whether they found tertiary authentication convenient. Convenience in the survey was used by the researchers as a stand-in for usability. However, this may not be how participants interpreted this word. Convenience for them may mean easily available as opposed to easy to use. Thus while 80% of participants agree that tertiary authentication is convenient,[13] the execution of the authentication scheme by platform operators and third-parties is a different matter.

Some of the inconveniences that participants felt when performing tertiary authentications were related to problems encountered while performing the quasi-experiment, as

[13] As per Question 3.

expressed in answers for **Q13**. For example, **P05** and **P08** wrote that they encountered some problems because they forgot some of their passwords. **P13** had a similar experience and added "*Keeping track of the various user names & passwords as I went back & forth was confusing. Specifically, I confused my Twitter account username with that of another I use occasionally.*" **P16** and **P17** experienced problems with the Facebook app on BlackBerry who would crash frequently.

Other inconveniences appear less related to the quasi-experiment and more typical of what users may encounter every day. **P09** wrote "*I had 2-step authentication that was causing difficulties, especially with Google on receiving code on the phone.*" **P19**, also responding to **Q13** wrote "*Hootsuite had some conflict between Twitter and Google and wouldn't work [.]*"

Q14: ten participants (50%) had concerns about the security of their information. Eight participants (40%) did not. **P9** wrote "*No, concerns. All details I don't want in public domain are not on Facebook, Google or Twitter.*" But **P18** had a different view. She wrote "*Yes, definitely because I am a private person and sometimes I do not want a circle of social network from one account view my things off another account.*" **P05** wrote "*I had concerns because I thought the apps were going to post things without my consent [.]*" **P10** commented the concerns about the security of her information "*It was certainly convenient. I felt a niggling thought that maybe I should be worried about security but then dismissed it.*" Participants may feel uncomfortable with tertiary authentication yet continue to use the practice. **P12** confirms this by writing *"...I continue to use them as I see fit.*"

Q15: when the answers of multiple participants are combined, limiting postings, adjusting privacy and security settings, and control over the devices and apps used were the preferred strategy for 65% of participants. Other popular strategies included changing passwords.

Q16: when the answers of multiple participants are combined, 8 participants (40%) suggested adjusting privacy and security settings when advising acquaintances about security when using Facebook, Google, and Twitter. Similarly, when multiple answers are combined, 7 participants (35%) suggested controlling what is posted in these platforms. Four participants (20%) suggested using multi-factor authentication and strong passwords.

This question was useful for verifying if participants perceptions and practices about tertiary authentication matched. Participants would want to provide third-parties better advice than the one they practiced. In fact, **P13** and **P20** wrote that their answers were the same as **Q15**. **Q19** wrote a similar answer to **Q15**. Many participants added new advices that were not covered in **Q15**. **P8** who mentioned no security measures for **Q15** wrote "□ *don't over share.* □ *have a uniform identity;*"

Q17: twelve participants (60%) felt that their information was safer because Instagram, Google Docs, and Vine are owned by Facebook, Google, or Twitter. Seven participants (35%) were unsure. Five participants (25%) disagreed. This question tested participants' perceptions of secondary authentication which is not fully analyzed in this research;

Q18: eight participants (40%) thought that their information from Instagram, Google Docs, and Vine was kept if they deleted their Facebook, Google, and Twitter account. This question tested participants' perceptions of secondary authentication which is not fully analyzed in this research;

Q19: thirteen participants (65%) thought that personal information collected by tertiary apps and services should be deleted if they delete their Facebook, Google, or Twitter accounts. Five participants (5%) thought that the information was kept. While **Q4** and **Q11** asked related questions about personal data deletion, this question tested how participants wanted tertiary apps to handle their data. Participants' responses were not just focused on what policy they wanted the platform operators to pursue but also on the difficulty of verifying that the information was deleted. This contrasts with **Q4** and **Q11** where participants felt that they had agency over their personal information. This question appears to have made many participants recognize the impasse. **P15** wrote "*They can't access platform login so platform info is gone but app info could still exist… but how can we login now to delete it if account is gone?*" From participants' responses, there is a sense that that 'someone' other than them should take care of personal data left behind automatically. This is a genuine request for greater convenience and usability to be embedded in platforms and tertiary apps for the benefit of user experience. **P11** response to the question was "*INSTANTLY "DISAPPEAR*." **P13** asked for a minimum of user convenience when she wrote "*You should at least be asked if you want it deleted or be given an option to create a new identity*."

A Participant reflecting upon the problem with data left behind with tertiary apps when deleting an account in **Q19** wrote *"[we] can't access platform login so platform info is gone but app info could still exist… but how can we login now to delete it if account is gone?*" Results for **Q19** demonstrate that 65% of participants think that their information collected independently by tertiary apps should be deleted. Twenty-five percent believe that their information stays. These results point to the same trends in **Q7** about how data coming from primary apps to tertiary apps is managed.

Q20: sixteen participants (80%) felt that security and confidentiality are not related concepts. **P19** wrote "*Security is about preventing access to account. Confidentiality is the guarantee that info won't be shared with 3rd party. Privacy: nobody can read my data. Pros and cons with 3rd party authentication. E.g. Google has better security for storing data than small developers, but you have to be careful to watch what you authorize.*"

5.3 Diagrammatic Mental Model Representations

To test if users' mental models about tertiary authentication differ from the design models used by platform operators I relied on two visual data collection methods. On one hand, I relied on participant-based diagrammatic-elicitations and then used researcher-produced photographic documentation to record the mental model representations drawn by the quasi-experiment's participants.

5.3.1 Researcher-Produced Photographic Documentation

Researcher-produced photographic documentation is a well-established visual research method used by biologists, physicists, sociologists, anthropologists and many other scientists in both hard and social sciences. Some scientists use this visual research method to document an objective reality of the world (Prosser and Loxley 2008). To do so, they repeat photographs of the same subject over time often to attempt to chronicle changes (Prosser and Loxley 2008).

After each task performed by participants during the quasi-experiment, I took photographs of the diagrammatic mental model representations that they produced. In this study, I use the photographs as documents recording the transient diagrammatic mental models' representations

that the research team erased after they were recorded by my camera. There is no attempt in this study to use reflexive or records of the procedures I used to produce the photograph as a qualitative data point. Still I briefly describe below a narrative of how I performed the photographic documentation.

The lights in the quasi-experiment room projected reflections on the white board used to hold the magnets in place. My research assistants and I tested several light settings for the room to avoid the light reflections which would create interference and noise that would prevent an appropriate reading of the diagrams. Shutting some of the lights did affect some participants with poorer eyesight. Turning the lights on and off would also distract participants adding unwanted intervening variables to the quasi-experiment. For most sessions with participants, the lights were left on. To avoid the white blob of light in the middle of the shot taken, I would position myself to isolate the reflections as best as possible. Since every diagram produced used space differently, I had no set position to take the photographs from.

Multiple shots were taken with the camera of my smartphone, a LG Nexus 4. The camera on the Nexus 4 is not the best in its category. The camera zoom, and aperture were often problematic and resulted in blurry shots. Some participants drew complex diagrams occupying a significant amount of the white board. Thus, I would take one large picture of the entire diagram, and then focus on groups of graphic objects in the composition. The last shot taken was always a photograph of the entire ensemble. Because each shot is automatically numbered by the camera, it allowed me to understand where a session started and ended when the photographs were transferred to a computer to be cleaned and processed.

Once transferred to a computer, a research assistant and I renamed all photographs following a strict nomenclature to allow us to understand which participant's diagram was photographed and which task was being documented. **Table 53** (in the Appendices) shows the nomenclature used for labelling the photographs. For clarification, 'Order of the Shot' per Session refers to the numeric order of the shot taken during the session with one participant. For example, if 43 shots were taken of the participant's diagrams in total, as per the example in **Table 53** in the Appendices, the shot was the second one taken during the session. 'Instance of the Shot per Task' refers to the order of the shot taken about a specific diagram representing a

task. In the **Table 53** example, the photograph was the first one taken of the diagram representing a specific task. Instead of using numbers to represent the order of the shot per task, I used alphabetical orders.

Multiple shots were taken including some that were discarded because they were unreadable by the computer and others which photographed the laboratory where the quasi-experiments were performed. Several shots were discarded as I used them as bookmarks to mark the beginning and end of a session. Many of these shots were photographs of packages of the snacks offered to participants. I kept 800 shots in all. Some were photographs of the mental models' tests that I asked participants to perform in the pre-task of the quasi-experiment. I soon abandoned the practice of photographing pre-task diagrams as this data was unnecessary for the evaluation. Towards the mid-point of the trials, I became more concerned with having backups and proper shots to choose from. I had discovered that some shots were corrupted, and others blurred. So, I began taking more than two shots per participants' diagrams. **Table 54** in the Appendices, shows the distribution of photographs per participants.

Once backed up, each relabelled photograph was parsed through a Photoshop script to equalize their levels and a copy was transferred from a 'raw' folder into a 'clean' folder. The level equalization was used to brighten the photographs. The photographs were not cropped, shrunk, or edited further. From the 'clean' folder, each photograph was then classified per task into a directory assigned to each participant. It is the photographs in these directories that were evaluated for this study.

Because only one white board was used by participants, after photographing each diagram after each task performed, my research assistant and I erased the diagrams produced by participants and reassigned the magnetic icons on the sides of the larger white board and to a smaller white board which was not used for diagramming. The smaller white board was used as a container for all extra magnetic icons. To facilitate participants' diagramming, the multiple instances of the Facebook, Google, and Twitter magnetic icons were kept on the larger white board.

Without the documentation of each diagram, there would be no records of participants' representations of their mental models. While the objectivity of the photographs can be challenged, their contribution to this study are as records of the diagrammatic mental model representations produced by the quasi-experiment's participants. I treat these photographs as legitimate, and valid record of the real object of interest of this study, which are the participants' diagrams.

5.3.2 Participant Diagrammatic-Elicitation

The diagrammatic mental model representation pioneered in this experiment extends diagram representation practices by using free-floating three-dimensional objects used in concert with traditional two-dimension graphics. I pre-fabricated magnetic icons representing the apps, platforms, and other components and instances of elements with which participants interacted with as they performed the quasi-experiment's tasks. **Figure 15** displays a sample diagrammatic-elicitation created by a participant.

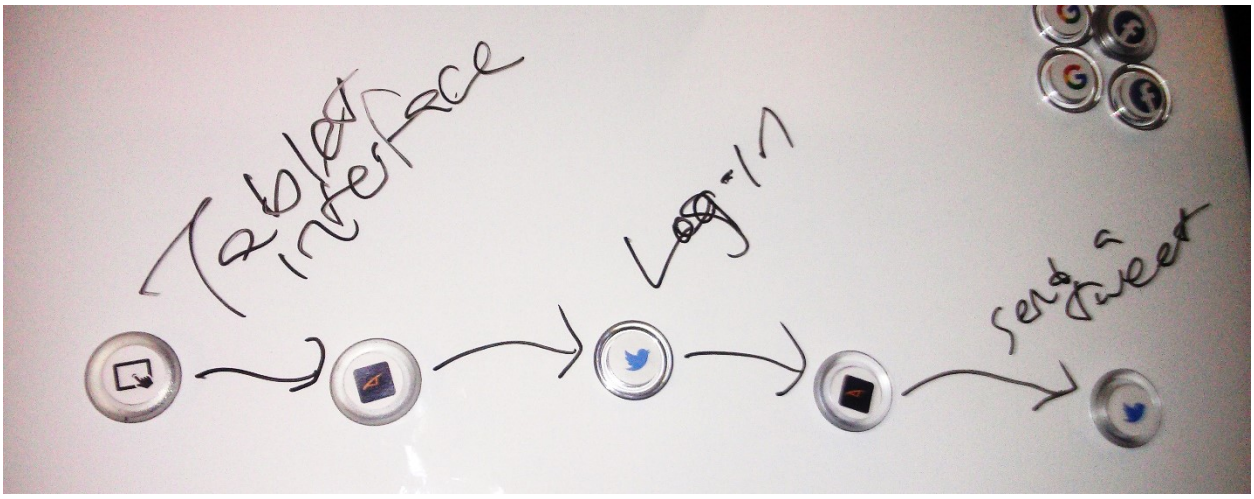

Figure 15 – P03 Sample Diagrammatic Representation

After each task, participants were instructed to represent their mental models of their interactions on a white board, using the magnetic icons, and felt pens. **Table 21** shows the exact instructions participants received verbally from me. I demonstrate the exact script for Task 5 below, but the apps and platforms used were changed for each question.

Table 21 - Diagrammatic-Elicitation Instructions

"Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with the Playbook Facebook app and Facebook? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task."

My research assistants and I used commercially available magnets used for white boards. The magnets are encased in a clear plastic buttons with larger top surfaces allowing the research team to apply stickers on them. The stickers were printed in colour with icons of the apps, services, platforms and several other elements and then applied to the surface. The stickers peel off easily from the surface of the magnets and had to be adjusted and reapplied throughout the conduct of the quasi-experiment between September and October 2016. The research team performed such maintenance before each session with a participant. While participants were often careful with the magnets, I do not foresee any negative variable affecting the conduct of the diagrammatic mental model representation and participants' interaction with the white board caused by the peeling off the stickers from the magnets.

Not all magnetic icons are created equal. We used a total of 70 magnets to represent 29 icons. During the quasi-experiment, we noticed that some terms should have been added or magnets could have been reassigned to other more used labels. For example, instead of the generic Google Docs magnetic icon, a Google Form magnetic icon would have been more appropriate. However, to maintain a constant experiment environment for all participants, there were no changes in the number and selection of magnetic icons presented to participants.

One innovation of the diagrammatic mental model representation method used in the quasi-experiment was the use of multimodal representations. Participants relied mainly on visual, tactile, gestural, and auditory modalities to draw diagrams of their mental models. Modalities in the context of HCI are often described as the ways in which people interact with technologies (McEwen and Dubé 2015; Sarroff 2008). There is an interaction process to modalities in that humans and computers can receive (input) and send (output) information. In the case of the diagrammatic-elicitation, participants did not interact with a computer or an electronic device that could respond to their inputs. It was a single use of a series of magnets, a white board, and drawing tools. Therefore, I refer to the diagrammatic-elicitations as multimodal representations.

Yet participants still used their vision to use the space and place the magnetic icons on the board. They used touch and gestures to control the felt pen, move the white board and the magnets. But participants also used their ears to perceive the clicking noise of the magnets adhering to the white board. While this seems obvious and perhaps trivial, I argue that the auditory response generated from putting a magnet on the white board was a wholly part of the experience of participants in the quasi-experiment.

Although not measured specifically, during the pilot and the quasi-experiment, the stickiness and play value of the magnets was observable. Play is a voluntary practice separating the player from her usual social life without compelling results being demanded of the person involved in active participation (Keenan 2016; Huizinga 1970; Suits 1978; Sutton-Smith 1997.[14] Part of the play value was created through the sounds produced by the magnetic icons. The sounds produced by the magnets are not responses from any artificial intelligence system and are no more responsive than the olfactory response participants obtained from the felt pen, or the visual stimuli from the diagrams drawn on the white board. Still the pulling the magnets from the board and fixating them in space did produce a limited amount of play value and satisfactory perceptions with a three-dimensional object.

Graphic representations are displayed in two-dimensional space even when their compositions exhibit three-dimensional space, like a 3D rendering seen on a computer monitor (Englehardt 2002). The monitor, which is the display medium is flat. Diagrams are a type of graphic representation which stand in between the verbal and pictorial representations (Englehardt 2002). They combine both elements of texts (verbal) and pictures.

Diagrams are composite graphic objects that convey relationships between some of their components (M. J. Umoquit, et al. 2011). The relationships conveyed are abstractions of complex ideas represented with an internal structure and notation system spatially (M. Umoquit, et al. 2013). The two main types of diagrams are concept maps and mind maps. They are used in

[14] I want to thank my colleague Andrew Keenan who shared his unpublished definition of play drawn from the cited literature.

research to demonstrate how people understand relationships between ideas (M. Umoquit, et al. 2013). Concept maps represent relationships hierarchically while mind maps represent links as non-hierarchical connections (Wheeldon and Faubert 2009).

Researchers have elicited concept maps and mind maps from participants to understand how they understand their mental models. Education scholars Sara McNeil and Larry Butts (2003) used concept maps drawn by a graduate student to measure their mental models about their multimedia learning processes. They compared the mental models of the student before he underwent a two-semester course on multimedia authoring and after. McNeil and Butts argue that concept maps represent only a snapshot of mental models at any given time and change frequently (2003).

Education scholar Shu-Nu Chang (2007) argues that conceptual models are analogous to conceptual maps. Chang bases his argument on the typology of mental models created by Johnson-Laird (1983) where the latter differentiates between physical models and conceptual models. Physical models, according to Johnson-Laird, are mental models that represent the physical world (1983, 422). Conceptual models are mental models that represent abstract ideas (1983, 422). Chang argues that conceptual maps can be expressions of mental models as they attempt to explain internal thinking frameworks.

O'Connor et al. (2008) used concept mapping with participants working in groups to represent shared levels of understanding between them. The researchers argue that concept maps can draw links around individual mental models and that this could be demonstrated through group activities (O'Connor, Johnson and Khalil 2008). Of interest to the researchers was how individual's mental models changed as they shared them with one another to create new concept maps.

In the three studies mentioned above where researchers used concept mapping to represent mental models, hierarchical orders between components was used. What was measured was the links between ideas. Concept and mind mapping approaches to operationalize mental models do work, but they are ill-suited for demonstrating a mix of physical and abstract ideas such as how platforms perform tertiary authentications.

Participants in this study were not asked to create purely abstracts models with definite hierarchies between ideas. Instead, following Clark's control point analysis which I have described several times in previous chapters, participants were asked to explain a sequential process that may contain hierarchical structures or not. The space that participants were asked to represent graphically is physical in the sense as it is part of the physical network of the Internet. But it is also abstract as data being passed around from one platform to another is not visible and more of an abstract idea.

The use of three-dimensional objects like the magnetic icons is interesting as it fixes abstract ideas about physical processes in space. While Facebook's server does occupy a physical space somewhere, the idea of Facebook as a virtual space may be an idea that exists only in participants' minds. With modalities such as touch, sounds, and smell, the diagrammatic-elicitation requested of participants, there is a play value that can enhance participants' recall and representation of their mental models that could not be replicated with typical concept and mind mapping techniques.

5.3.2.1 Qualitative Summary of Diagrammatic Representations

I performed a qualitative review of each task performed by each participant. These reviews were used to familiarize myself with the output and start developing a language for evaluating the participants' diagrams. The sample questions were developed from a grounded theory approach (Corbin and Strauss 1990) where I began to record patterns in participants' diagrams. Once refined into the six questions, I went back to earlier questions and reviewed them all with the same questions. In each evaluation, I asked the following questions as seen in **Table 22.**

Table 22 - Qualitative Summary of Diagrammatic Representations Questions

Is there a login?
Is there a log out?
Which devices were used in the tasks?
Which steps were covered or not?
Relationships between primary, secondary and tertiary indicated?
Reaction to access rights requested?

For each task evaluation, I wrote descriptions about which icon appeared first to understand the interaction path. **Table 23** contains sample descriptions from a few participants' diagrams.

Table 23 - Sample Qualitative Descriptions

P03	**Task 6**	Depicted the laptop icon. Then Twitter to log in. Then the keyboards and another icon for sending a tweet. No log out.
P11	**Task 5**	The Blackberry icon is followed by the keyboard icon and then Facebook. No login, access rights or tasks are depicted.
P19	**Task 11**	The Firefox icon connects to a keyboard icon. It also connects to the Internet icon which then connects to a Google icon. The Google icon connects to a mouse icon and a custom Google Plus icon.

Then, I wrote a summary of the most salient points based on the six questions below. **Table 56** in the Appendices contains the summary participants' diagrammatic representations.

5.3.2.2 Qualitative Summary of Mental Models

The qualitative summary of the mental models is a more elaborate qualitative analysis of the diagrams that is less concerned with the mechanics of the diagrams and more with their meaning and what can be intuited from them. Each diagram was analyzed, and a summary of the most salient points was then written. **Table 57** in the Appendices contains the summary of the mental models.

5.3.2.3 Diagrammatic Representation Metrics

To interpret the data contained in the participant-elicited diagrammatic representations, I introduced a series of measurements that do not focus on the qualitative aspects of the output. **Table 24** contains a descriptive summary of the diagrammatic-elicitations produced by participants. The metrics include all 15 tasks performed by all 20 participants. This includes primary, secondary, and tertiary authentications.

Table 24 - Descriptive Summary of Diagrammatic Representations Metrics

Statistics

		Number of Icons	Duplicate Icons	Diagram Complexity	Written Complexity	Errors
N	Valid	300	300	300	300	300
	Missing	0	0	0	0	0
Mean		4.66	1.45	2.19	2.06	0.07
Median		5.00	0.00	2.00	2.00	0.00
Mode		3	0	2	2	0
Std. Deviation		2.313	1.818	0.609	0.743	0.286

Variance	5.349	3.305	0.371	0.552	0.082
Minimum	0	0	1	1	0
Maximum	15	10	3	3	2
Sum	1398	434	658	618	22

The first metric introduced is the 'number of icons'. Each participant used different numbers of magnetic icons in their diagrams. To represent a tertiary authentication, at least two magnetic icons are necessary. The first is for the tertiary app. The second is for the primary platform. If modalities of interactions are used, it could increase the number of magnetic icons to three. However, in practice, participants use more than two magnetic icons. For example, for some tasks, **P18** used no magnetic icons. **P10** used a maximum of 15 magnetic icons for some tasks as can be seen in Figure 16.

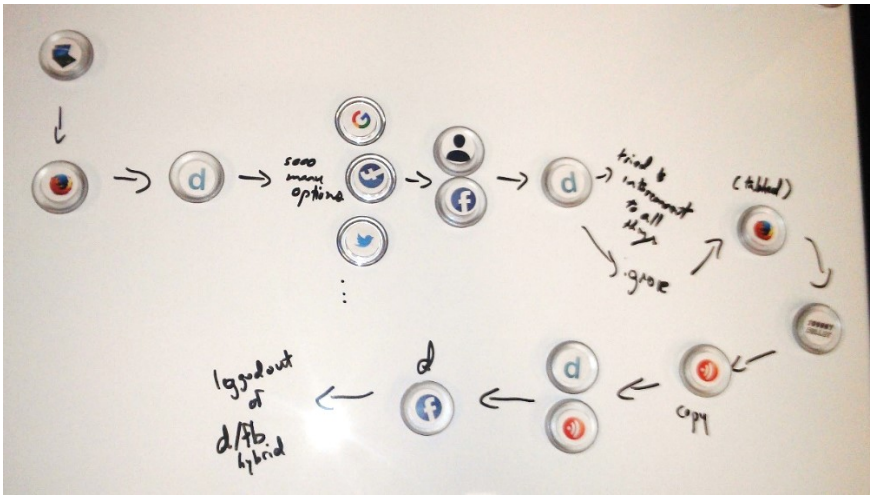

Figure 16 - High Number of Magnetic Icons Used (P10)

If every icon represents a point of interaction, the numbers used help understand how participants perceived their interaction. However, the number of icons should not be used as a rule. While using each magnetic icon as a point of interaction appeared to be the norm, for **P18**'s diagrams, it was irrelevant. In many diagrams, **P18** used magnetic icons not as sites of interaction but as logos for the apps' whose interaction she was representing. For example, as can be seen in **Figure 17**, the diagrammatic representation of Task 5 which involved tertiary authentication with Facebook app for the Blackberry Playbook, the Facebook magnetic icon is used as a logo. The line illustrations appear to depict a tablet containing the Facebook app. An

extra tablet icon is used to depict the modality of interaction (a hand gesture) used to interact with the tablet.

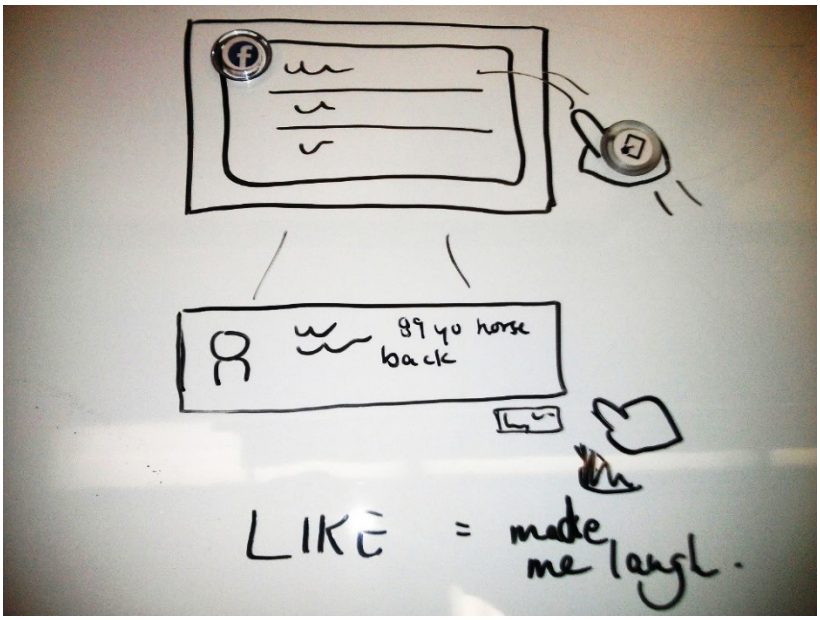

Figure 17 - Icons used as Logo (P18)

In a few more diagrams **P18** did not use any icons to represent her mental models. For example, in her diagrammatic representation of the tertiary authentication with Facebook into AngryBirds Friends, no magnetic icons were used as sites of interaction nor as logos as can be seen in **Figure 18**.

Figure 18 - Diagram without Magnetic Icon (P18)

Similarly, the number of duplicate magnetic icons helps us understand how many times a participant perceived an interaction with a specific point of interaction, as represented by a magnetic icon. As stated in **Figure 14**, Facebook, Google, and Twitter had six magnetic icons each. Other apps and services had three or less magnetic icons. **P04**, **P05**, **P06**, and **P12** did not use any duplicate magnetic icons. In some cases, these participants used other schemes, like looping lines or arrows stemming from one app to represent multiple interactions with one site of interaction. These representations use less linear and sequential thinking in the generation of mental model representation. **P10** used 10 duplicate magnetic icons. As noted above, **P10** used more magnetic icons than other participants. The number of duplicate icons increases the total number of icons used.

Another metric introduced was Diagrammatic Complexity. Diagrammatic complexity seeks to measure the complexity of diagrams represented by participants. The use of diagrammatic complexity as used in this study is not a novel idea. Cognitive styles of users' mental models have been linked to their spatial and verbal ability (Hockey 1990). Participants' technical literacy and education differed. Diagrams require a high level of abstract thinking as ideas, phenomena, and their relationships are represented. I used a simple table to assess the

diagrammatic complexity of each diagram created by participants. **Table 25** includes the whole scale.

Table 25 - Diagrammatic Complexity Scale

DIAGRAMMATIC COMPLEXITY SCALE	
1	No directional arrows, links or graphic objects
2	Used directional Arrows
3	Created New Icons and Graphics

Diagrams that did not use any directional arrows, links or other graphic objects apart from the magnetic icons were rated 1. For example, in **Table 26**, the mean of diagrammatic complexity of **P04**'s 15 tasks is 1.13. As seen in **Figure 19**, the participant used directional arrows rarely, preferring to line up icons next to one another and hinting at invisible links between them.

Table 26 - Participant 4 Diagram Complexity

P04	Metrics	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	Mean	Median	Mode
	Diagram Complexity (1-3)	1	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1.133333	1	1

Figure 19 – P04 Sample Diagrammatic Representation

Diagrams with diagrammatic graphic objects such as directional arrows were given a complexity rating of 2. When participants created new icons apart of the magnetic icons available and added graphic objects unrelated to linking, I rated the diagrammatic complexity at

3. **Figure 20** shows the diagrammatic complexity of **P14**, who along with **P18**, had a mean and a median complexity rate of 3.

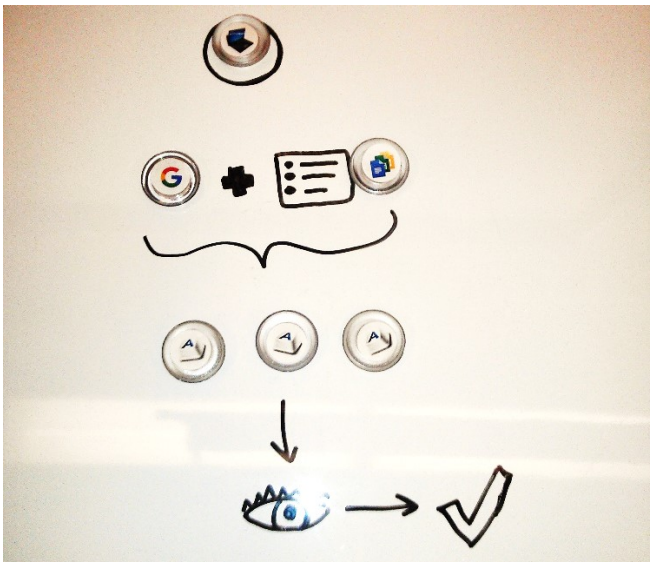

Figure 20 - P14 Sample Diagrammatic Representation

While some participants such as **P04** seldom used diagrammatic graphic objects, they annotated their diagrams with written annotations extensively, as seen in **Figure 21**.

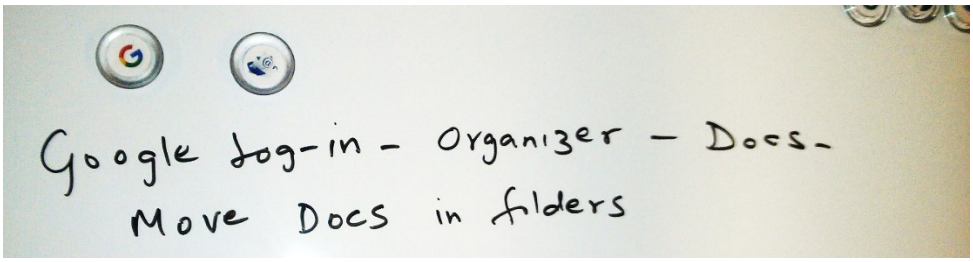

Figure 21 – P04 Diagrammatic Annotations

A complexity scale for written annotations was also introduced to better understand participants' diagrams. To develop a complexity scale specific to the diagrammatic elicitation used in the quasi-experiment, I drew from the literature on visual language research, and linguistics. Visual language researcher Yuri von Englehardt (2002) describes words included in diagrams as non-pictorial graphic objects where written texts' organization within a graphic composition are influenced by the grammar, and the syntax of the language expressed.

However, Englehardt's taxonomy does not address the complexity of written graphic objects. Linguists Rod Ellis and Fangyuan Yuan (2004) have developed metrics to analyze written texts based on similar approaches used for the evaluation of oral languages. Syntactic complexity measures include syntactic complexity, syntactic variety, and the Mean Segmental Type-Token Ratio (MSTTR) (Ellis and Yuan 2004). Syntactic complexity measures the ratio between clauses and T-units (Ellis and Yuan 2004), which are defined as a main clause and others depending on the first (Foster, Tonkyn and Wigglesworth 2000). Syntactic variety measures how many different grammatical verb forms are used in one utterance (Ellis and Yuan 2004). MSTTR is a calculation used to remove the variance problems created by differing sample sizes between participants (Malvern and Richards 2002).

To further understand the complexity of written texts as used in the quasi-experiments, we must consider their spatial representation and as aspects of the participants mental models. Neuroscientist David Kemmerer (2006) explores the interaction between language and the perceptual/cognitive representation of space in a literature review of the neuroscience research. He argues that non-linguistic mental processes about space appear to be separate from spatial categorization systems of world languages (Kemmerer 2006). Yet, he also notes that the literature supports the conflicting idea that the native language of a speaker does have influence on the perceptual and cognitive categorization of space (Kemmerer 2006).

Linguists Annette Kerskovits (Kerskovits 1986) writes that the spatial representation of words is at best an inadequate approximation of reality using a person's native space in linguistic rules to create semantic representations of an idealized world.

Based on the literature discussed above, I have created as simple complexity scale for evaluating participant's written annotations within diagrams. Participants were not asked to use written annotations to draw graphic elements or even forced to use the magnetic icons. Hence the classification used in this study is developed from the results obtained from participants' diagrammatic elicitations. Some participants used no written annotations. Some used short words, and some used full sentences. **Table 27** displays the Written Annotation Complexity Scale.

Similarly, to the Diagrammatic Complexity Scale, I used a three-level ordinal rating system to measure the complexity of the written annotations included in participants' diagrams. The rating for diagrams without any written annotations is 1. The rating for diagrams with short descriptive tags is 2. These tags would rank below a T-unit as defined by Ellis and Yuan (2004), and Foster, et al. (2000). The rating for diagrams with full sentences and longer annotations is 3. Full sentences are equivalent for full T-units but there was no need to further quantify them using a MSTTR or a syntactic variety metric.

Table 27 - Written Annotation Complexity Scale

WRITTEN ANNOTATION COMPLEXITY SCALE	
1	No written annotation
2	Short descriptive tags
3	Wrote entire sentences

The evaluation of ratings between 2 and 3 was often difficult to determine as participants used a variety of representation schemas. I was the sole coding researcher for the Written Annotation Complexity Scale. In **Figure 19**, I rated **P04**'s diagram at 3 while rating **P07** at 2. **Figure 22** displays a sample diagram from **P07** rated at 2.

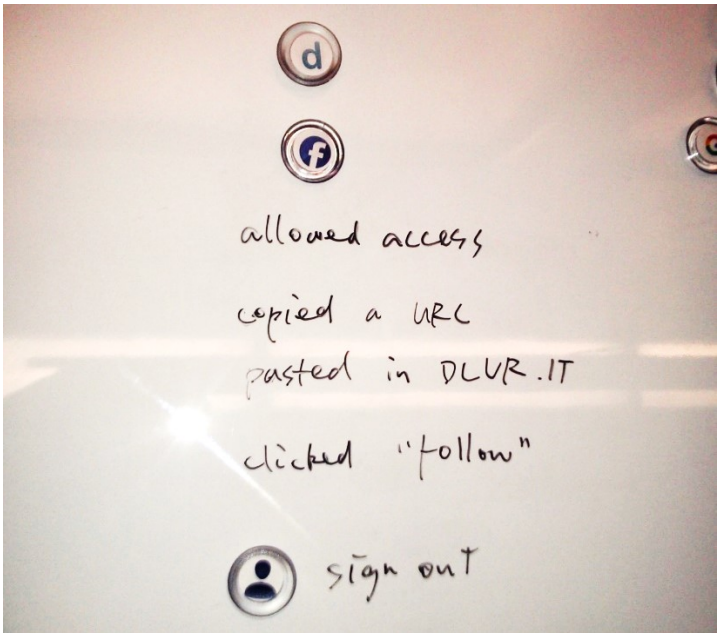

Figure 22 – P07 Sample Diagrammatic Representation

The last metric I used to evaluate participants diagrammatic-elicitations was the Error/Correction measurement. This measurement is critical for the evaluation of the variances between their mental models and their representations. Because mental models live in people's minds representing them means that information will be changed and altered by participants. Moreover, how participants recall their actions may differ from their actual mental models. Although difficult to evaluate, I propose the measurement of errors and corrections on the white board as possible demonstrations of breaking points between participants' mental models and their representations.

The measurement of errors and corrections was difficult to assess in some cases. While **P01** was discouraged from erasing his diagrams, he continued to erase, smudge and redo many of his diagrams. Afterward, I strongly discouraged every other participant to not erase or smudge graphic elements that they disproved. They were instructed to cross unwanted graphic elements so that it was clear that they were errors corrected elsewhere. While drawn graphic objects like texts and directional arrows can be measured with the Error/Correction metric, this measurement cannot account for magnetic icons being moved by participants reassessing their mental model representations. **Figure 23** displays a sample diagram from Participant 1 where he attempted to correct errors.

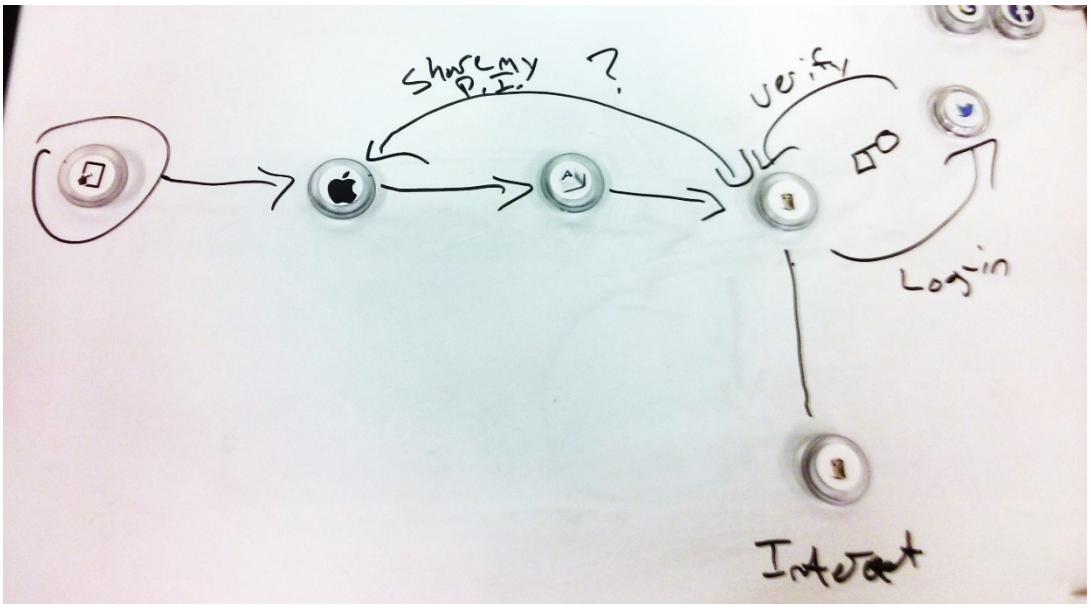

Figure 23 – P01 Sample Diagrammatic Representation

5.3.2.4 Diagrammatic Representations Coding

I based my analysis of the diagrams on 14 questions (or themes) drawn from the data that I collected during the qualitative summaries of the diagrammatic representations and the mental models. Again, a grounded theory approach (Corbin and Strauss 1990) influenced the generation of the 14 questions. These questions allow me to operationalize and quantify an understanding of the diagrams and their meanings. They also helped me formulate a strategy to test conjecture 1 which argues that people's mental models about how tertiary authentication works differ from platform operators' design models. The primary and secondary authentications which were also collected we not evaluated for this study. **Table 28** includes the list of questions drawn from observed themes.

Table 28 - List of Questions Drawn from Themes

Is there a login?
Is there a log out (PC) or exit from app (mobile)?
Are there modalities of interactions?
Are the modalities in the interaction path?
Relationships between primary, secondary and tertiary indicated?
Reaction to access rights requested?
Is it a linear interaction path?
Abstract or physical Model?
Are there pairs as sites of interaction?
Does the primary platform precede the tertiary authentication?
Is the tertiary authentication part of the interaction path?
Differentiation of the operating system from the device (mobile), the browser from the PC (PC), or Indication of independent Internet (both).
What or where is the initial site of interaction?
What is the last site of interaction?

A 15th question "Is there a difference for initial site of interaction when on the table versus the laptop?" was discarded. It was easy to achieve the same answer by comparing questions 13 and 14 if needed. It turns out that the data revealed by **Q15** was not as relevant. It sought to compare participants' interactions when using laptops versus mobile devices. The study did not control for differences in interaction between sites of interactions. Any data revealed would have supported the conjectures superficially.

The analysis of the 14 questions was based on simple codes. Twelve of the 14 questions were coded with binary codes. Questions 1,2,3,4,5,6,7, 9, 10, 11, and 12 were yes or no questions. Question 8 was based a binary code based on specific terms – abstract or physical. Questions 13 and 14 were coded using sites of interaction as options. Thus, the possible codes were limited to apps, platforms, and devices used by participants in their diagrams. **Table 29** has a summary of the coding used.

Table 29 - Types of Coding Used

QUESTION	1	2	3	4	5	6	7	8	9	10	11	12	13	14
CODES	0/1	0/1	0/1	0/1	0/1	0/1	0/1	Abstract/physical	0/1	0/1	0/1	0/1	open	open

Four additional coders not involved with the research helped review every diagram. Each coder was a graduate student at the University of Toronto and had adequate mastery of English when it was not their native language. **Table 55** in the Appendices describes the coders' backgrounds. The coders were acquaintances.

Each coder looked at each task and assigned it a verbal code that I recorded. They were not directly made aware of the previous codes that I had produced. To avoid possible learning biases per platform, the additional coders were assigned reviews with Facebook, Google, and Twitter. They were not assigned two reviews with only one platform. When disagreement over my coding occurred, I would notify them. There were between 2-6 disagreements per tasks analyses from a total of 280 analyzed tasks. There was a total of 2520 tasks analyzed. **Table 30** explains some of the disagreement metrics used to calculate Equation 1 which analyzes the disagreement rate between coders.

Table 30 - Disagreement Metrics

Diagrams per Tasks (i.e., one tertiary authentication)	280 (14 questions x 20 participants)
Disagreements per Tasks	2-6
Total Number of Tertiary Tasks Evaluated	9
280 x 9 (Total Number of Trials)	2,520
280 - 6 (Maximum potential disagreement)	274
274 x 9 (Number of Successful Trials)	2,466

A major claim of this research project is that the diagrammatic elicitation of participants' mental models used can yield valid, reliable, and legitimate results about how people perceive their security, confidentiality, and privacy as they perform tertiary authentications. Therefore, the rate of agreement about the coding based on the 14 questions matters. As seen in **Table 30**, the number of disagreements per task was between 2 and 6 for each column. By using the maximum number of disagreements between coders, it is possible to determine the success probability of the coding. If using the total number of success (or agreements, in the context of the study) using a simple equation, the probability of success can be determined. The probability of success is about 98% (when rounded-off).

Equation 1 - Probability of Success. Values for K and n are from Table 13

$$\text{Probability of Success (P)} = \frac{\text{Number of Success (K)}}{\text{Number of Trials (n)}}$$

$$P = \frac{K}{n} \qquad 0.978 = \frac{2{,}466}{2{,}520}$$

Probability of Success = 0.978

In some cases, we would discuss these cases briefly. In some cases, the coders' input corrected errors that I had produced because of fatigue. Errors would occur about twice per tasks reviewed. In such instances, the corrected codes were adjusted directly. In more problematic cases when disagreements happened, we moved ahead and returned to them after all the initial coding was done to discuss them fully. In many instances, the coders' understanding of my decisions which they had disagreed with originally changed after having reviewed all the tasks. With more experience, they could see why I had made some coding decisions. A few times, it was necessary to view participants' diagrams of primary and secondary authentications to understand their patterns of mental model representations.

When disagreements persisted, several diagrams from the same participants were reviewed at once to understand their diagrammatic representation patterns. Precedents agreed

upon in past reviews with earlier coders were also used to inform newer reviews. In some challenging instances where no agreements were reached between individual coders and me, a third coder was invited to verify the codes. When all tasks are combined, there were only 4 cases requiring a third coder to review the code. These cases were left for last with all coders. After reviewing the code independently, the first coder and I would present our case which the third coder voted on. The third coder's decision was used as the final decision.

5.3.2.4.1 Is there a login?

This question asks if participants actively represented an authentication process. It tests for awareness of authentication as a major step in the person's mental model. This question matters because every participant was presented with a tertiary application with which theoretically,[15] they had had no prior relationship with. To use them, participants had to perform a primary authentication that would verify their identity and then allow them to pass the necessary personal information to access the tertiary application. As can be seen in **Table 58** (in the Appendices), although results vary per tasks, most participants represented logins and thus were consciously aware of logins as a part of the tasks they were performing. Participants whose diagrammatic responses were coded 'no' did not represent a login. Those coded 'yes' did.

While the lack of representation of a login does not indicate that the participant was not aware that that an authentication took place, it does suggest whether it was not a significant action that mattered to them. The results per tertiary apps do differ. Looking at participants' diagrams for dlvr.it and Hootsuite, only **P18** did not represent any login. **P18** did not represent a login because her diagrams were abstracts as discussed below and thus did not necessarily represent a physical reality. **Figure 24** represents **P18**'s diagram for dlvr.it. In her diagram, the linear path of interaction is also missing. As will be explained below, without a linear path of interaction, there are no linear steps per say. The participant focused more on representing a situation rather than a process.

[15] Although as recruitment condition to participate in the study, as mentioned in the Research Approach Chapter, some participants did not fully disclose that they had used some of the tertiary apps previously. Others had forgotten that they had attempted to create accounts with them in the past.

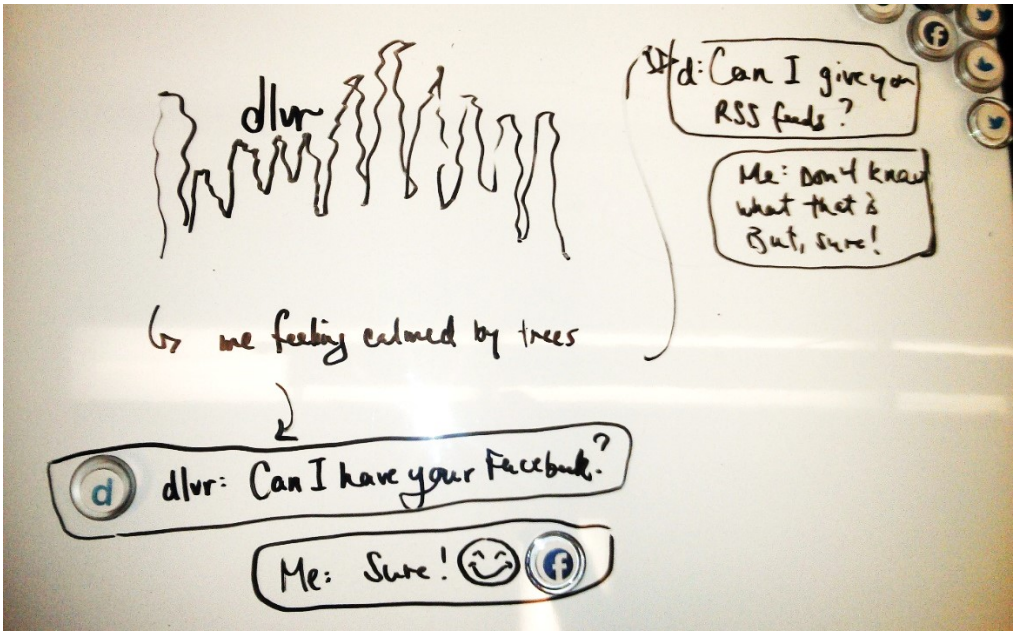

Figure 24 - P18's dlvr.it Diagram

Figure 25 represents **P18**'s diagram for Hootsuite. Again, there is no path of interaction as the participant did not represent a process but focused on representing a situation. Except for **P18** who is an outlier who focuses on situational representations rather than procedural ones, every other participant represented a login in their diagrams for dlvr.it and Hootsuite. This was not the case for other tertiary apps.

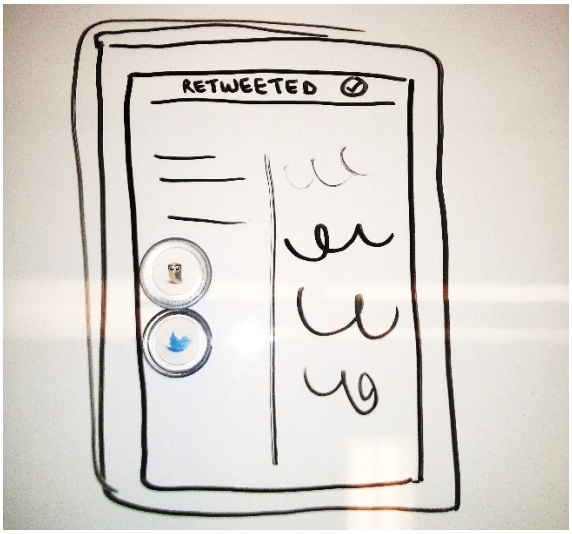

Figure 25 - P18's Hootsuite Diagram

As seen in **Table 58**, authentication using Facebook as a primary platform and AngryBirds Friends and Facebook for the Blackberry Playbook as tertiary apps obtained higher numbers of logins represented in diagrams. Both AngryBirds Friends and Facebook for the Playbook have different modes on interaction than other tertiary apps. To play AngryBirds Friends, the user is still within the Facebook environment. While the game is a tertiary app, it exists in the context of the Facebook platform. Users can navigate to other parts of Facebook, open the game in a separate browser tab, or return to the game as they wish. In the case of Facebook for the Blackberry Playbook it is possible that many participants felt that the app was from Facebook. In fact, there were no separate magnetic icons for participants to represent the Facebook Playbook app.

In the case of AngryBirds Friends, six participants did not represent a login. Each of these six participants did not represent a login with the Facebook Blackberry Playbook app either. Overall these six participants (P05, P06, P08, P12, P14 and P18) tended to represent logins less than other participants. In the 9 tertiary authentication tasks, they represented logins between 1 and 7 times. As can be seen in **Table 31** other participants represented logins between 9 and 8 times. Hence, participants who represented a login for AngryBirds Friends and Facebook Blackberry Playbook tended to represent logins regardless of the tertiary app represented in a diagram. Of the six participants who tended to not represent logins, four were women between 18-34 but I doubt that there are any correlations with these demographic features. Neither do I observe any correlations with the conditions tested in experiment.

Based on these results, I argue that participants are aware of logins most of the time or not. If authentications are part of participants' mental models as they interact with information systems, they represent them in diagrams. For a sizable minority of participants, authentications are not elements worth representing and thus not part of their interactions with platforms and tertiary apps. At most, authentication is an adjunct function that interfere with their interactions with information systems. A similar argument has been made by usable security scholar Ka-Ping Yee (2002) about the secondary place security occupies in users' mind.

Table 31 - Logins Representation Details

PARTICIPANTS	T3A	T4B	T5C	T8A	T9B	T10C	T13A	T14B	T15C	TOTAL	AGE RANGE	GENDER	SCENARIO
P01	1	1	1	1	1	1	1	1	1	9	25-34	Male	yes/yes
P02	1	1	1	1	1	1	1	1	1	9	35-44	Male	yes/ no
P03	1	1	1	1	1	1	1	1	1	9	25-34	Male	no/yes
P04	1	1	1	1	1	1	1	1	1	9	55-64	Female	no/no
P05	0	1	0	1	0	1	0	1	0	4	18-24	Female	no/no
P06	0	1	0	1	1	1	1	1	1	7	25-34	Male	no/no
P07	1	1	1	1	1	1	1	1	1	9	35-44	Female	no/yes
P08	0	1	0	1	1	0	0	1	0	4	25-34	Female	yes/yes
P09	1	1	1	1	1	1	1	1	1	9	25-34	Male	yes/yes
P10	1	1	0	1	1	1	1	1	1	8	25-34	Female	yes/no
P11	1	1	1	1	1	1	1	1	1	9	65+	Female	no/yes
P12	0	1	0	1	0	1	1	1	1	6	25-34	Female	yes/yes
P13	1	1	0	1	1	1	1	1	1	8	55-64	Female	yes/no
P14	0	1	0	1	1	1	1	1	1	7	18-24	Male	yes/no
P15	1	1	1	1	1	1	1	1	1	9	25-34	Male	no/yes
P16	1	1	1	1	1	1	1	1	1	9	18-24	Female	yes/yes
P17	1	1	1	1	1	1	1	1	1	9	55-64	Male	no/no
P18	0	0	0	0	0	0	0	1	0	1	18-24	Female	yes/no
P19	1	1	1	1	1	1	1	1	1	9	18-24	Male	no/yes
P20	1	1	0	1	1	1	1	1	1	8	25-34	Male	no/no

5.3.2.4.2 What is the Exit?

This question asks if the participant actively represented the end of a session either by logout of a session of the laptop or by shutting or pushing an app aside on the tablets. This question is based on the concept of the ephemeral technology introduced in the transactional token theoretical framework. As argued earlier, ephemeral technologies provide users with sessions. User interaction with these technologies are finite. Once the user logs out, their lack of authentication prevents access to the ephemeral technology as individuals whose identity is verified. This question measures if participants were actively aware or concerned about ending an authenticated session with a primary platform and a tertiary app.

Observing the diagrams, it became apparent that for some users the representation of the end of a session was not as important as the login process. As seen in **Table 59** (in the Appendices), in every task, most participants did not represent the exit from a session, even though they were instructed to when each sets of instructions were read to them during the quasi-experiment.

However, when observing the cumulative statistics of logouts representations reveal another story is revealed as per **Table 32**. A strong minority of participants did not represent

logouts. There appears to be no correlation with being part of the test or control group, gender, or age. There is no correlation with participants who represent their diagram abstractly or physically, as seen in the Model column which includes a cumulative count of physical mental models.

Table 32 - Logouts Representation Details

PARTICIPANT	T3A	T4B	T5C	T8A	T9B	T10C	T13A	T14B	T15C	TOTAL	AGE	GENDER	SCENARIO	MODEL
P01	0	0	0	0	0	0	0	0	0	0	25-34	Male	yes/yes	9
P02	1	1	0	1	1	1	0	0	1	6	35-44	Male	yes/ no	8
P03	0	0	0	0	0	0	0	0	0	0	25-34	Male	no/yes	8
P04	0	0	0	0	0	0	0	1	0	1	55-64	Female	no/no	1
P05	0	0	0	0	0	0	0	0	0	0	18-24	Female	no/no	7
P06	1	1	1	1	1	1	1	1	1	9	25-34	Male	no/no	0
P07	1	1	1	1	0	1	1	1	1	8	35-44	Female	no/yes	0
P08	0	0	0	0	0	0	0	0	0	0	25-34	Female	yes/yes	8
P09	1	1	1	1	1	1	0	0	0	6	25-34	Male	yes/yes	9
P10	1	1	0	1	1	0	1	1	0	6	25-34	Female	yes/no	9
P11	1	1	0	0	0	1	0	0	0	3	65+	Female	no/yes	8
P12	0	0	0	0	0	0	0	0	0	0	25-34	Female	yes/yes	8
P13	0	0	1	0	0	1	0	0	0	2	55-64	Female	yes/no	9
P14	0	0	0	0	0	0	0	0	0	0	18-24	Male	yes/no	4
P15	1	1	1	1	1	1	1	1	1	9	25-34	Male	no/yes	6
P16	0	0	0	0	1	0	0	0	1	2	18-24	Female	yes/yes	9
P17	1	1	1	1	1	1	1	1	1	9	55-64	Male	no/no	9
P18	0	0	0	0	0	0	0	0	0	0	18-24	Female	yes/no	2
P19	0	0	0	0	0	0	0	0	0	0	18-24	Male	no/yes	9
P20	0	0	0	0	0	0	0	0	0	0	25-34	Male	no/no	6

These conflicting results can be explained by looking closely at three groups of participants. Group A (P01, P03, P05, P08, P12, P14, P18, P19, and P20) never represented logouts in their diagrams. Group B (P06, P15, and P17) always represented logouts in their diagrams. Finally, Group C (P02, P04, P07, P09, P10, P11, P13, and P16) represented logouts at various rates. It appears that the representation of logouts is indicative of how participants perceive the authentication process and is thus something that is part of their mental models or not outside of the conditions used to test their perceptions in the quasi-experiment. When revisiting the cumulative count of physical models of Group C, only **P07** represents her diagrams abstractly. Yet only one of **P07**'s diagrams does not represent a logout. The majority of **P04**'s diagrams about tertiary authentication are also abstract, except for one. Within Group C, other participants generated abstract or mental models based on the situation presented. I argue that their mental models varied and did not systematically account for authentication. They could have forgotten to represent this or found it irrelevant in the diagrams where this was omitted. It

also appears that there is a strong correlation between the representation of abstract or physical mental models and the representation of logouts in diagrams. I explore the contrast between abstract and physical mental models further in one of the thematic questions below.

5.3.2.4.3 Are there modalities of interactions?

Modalities of interactions refers to the input and output used by users to interact with the platforms and the tertiary apps and services. The two modalities represented by magnetic icons were the keyboard and the mouse. However, some participants drew hands for gestures used on tablets or indicated taps in their annotations. The presence or omission of modalities of interaction helps explain how participants perceive their interactions with platforms and apps. Often, they used the modalities to represent the act of entering account information while performing an authentication. For example, **P10** writes "*Log in was easier on laptop & iPad since I am familiar but liked logging in on Android – flowed nicely. I did not like apps that overwhelmed with log in options like dlvr – invasive feeling.*" **P12** found authentication with tablets more difficult in part because of the modality of interaction. She shared this observation this. "*It's harder to login with tablets because of the touchscreen keyboard.*"

The use of modalities of interactions as seen in **Table 60** (in the Appendices) is almost even in many of the tasks. Some users use them consistently. Some do not. While it may shed some light about how they represent their mental models, the use of modalities in diagrammatic representations does not seem to be a variable affected by participants' perceptions of privacy, security and confidentiality. Instead, it appears to be something about how they perceive the world in general.

5.3.2.4.4 Are the modalities on the interaction path?

While evaluating the diagrammatic representations, I noticed that modalities of interaction may or may not be part of the interaction path. Including modalities in the interaction path or not indicates specific perceptions about how interaction is performed. Is a modality for a participant an element within or outside of the site of interaction? **Figure 26** has a sample from **P01** where modalities are part of the interaction path. In the sample, the keyboard is used in the interaction path.

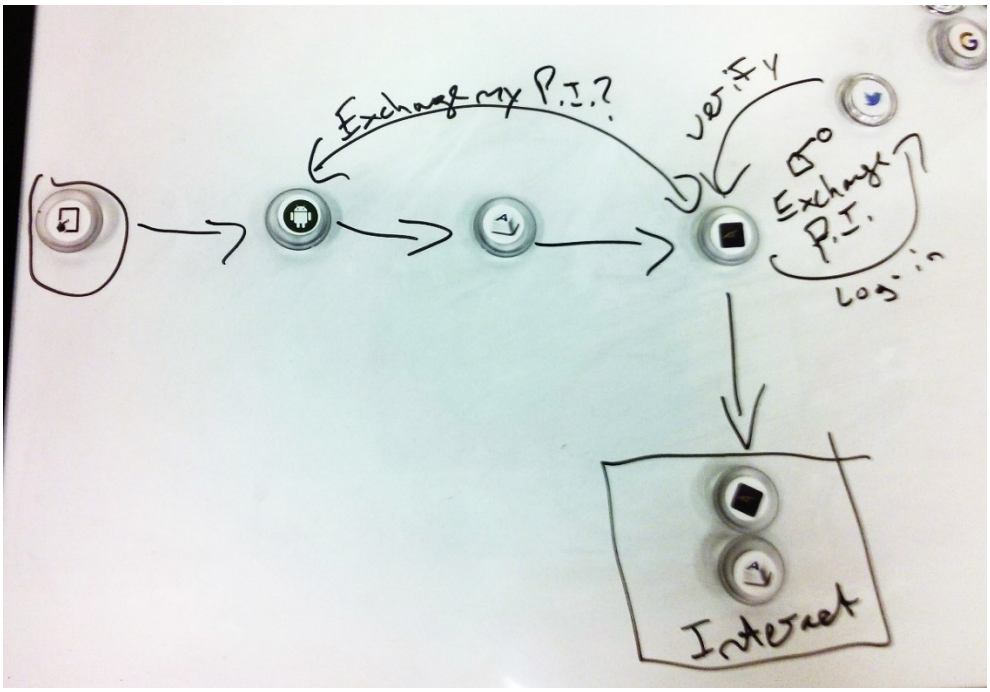

Figure 26 - Modalities in Interaction Path (P01)

The results must be considered in light of the previous questions. Only participants who answered yes in the previous question can answer positively here. This is reflected by the greater amount of negative answers.

5.3.2.4.5 Relationships between primary and tertiary indicated?

This question measures if participants indicated a relationship between the primary platforms and tertiary apps or services. As seen in participant's responses to the questionnaire, the relationship between primary platforms and tertiary apps seems to be something people are conscious of whether they react to it actively or passively. **P18** writes *"...I am a private person and sometimes I do not want a circle of social network from one account view my things off another account.*" **P14** appreciates the convenience (usability) of the relationship between primary platform and tertiary apps and although claims to have no concerns, mentions some. He writes "*No concerns. It makes it very easy. My concern is always w/ the apps posting to my page w/o consent but I can see there are settings to disable that.*" **P12** admits that tertiary authentication is a common practice but continues to use this method regardless of concerns when she writes "*Generally way [sic] of logging into any app, but I continue to use them as I see*

fit." **P15** expresses discontent with tertiary authentication prompts from primary platforms and actively attempts to control the relationship with tertiary apps. He writes that he *"... [Limits] access as much as ... desired.*" He specifically criticizes the practice of requesting personal information through tertiary authentication while forcing users to duplicate and recreate an account with the tertiary app. He writes "*I don't like when a platform login is requested then I still have to create a new username or password, so why did I give them credentials? – Dropbox*(.)" **P09** and **P13** attempt to control the relationship between primary platforms and tertiary apps by limiting what the former has access to, thereby reducing the risk for personal information to flow from one information system to another. **P09** writes *"...All details I don't want in public domain are not on Facebook, Google or Twitter.*" **P13** reveals that she "*[tries] to keep personal info off those platforms to minimize security issues."*

Being on the same interaction path is not a sufficient display of relationship. Relationship entails interaction by both parties such as a loop. A relationship can also be represented by a clearly indicated result produced from the relationship between the primary and the tertiary apps. In some diagrams, like with the BlackBerry, there were no differentiation between the primary platform and the tertiary. At the other end, such as Dropbox, every participant indicated a relationship between the primary and the secondary. **Table 62** (in the Appendices) contains the results for this question.

5.3.2.4.6 Reaction to requested access rights?

If there is no relationship between primary and tertiary apps, there should be no reaction to access rights. This question is important to evaluate participants' awareness of security, confidentiality, and privacy as they performed tertiary authentications.

Some participants noted in their diagrammatic representations their reactions to tertiary apps and services asking them for access right to their primary platform accounts. In his questionnaire responses, **P15** asserted that tertiary apps had "*(d)ifferent options for what info they wanted to access from the platform. Did they really need it?*" P03 found that "(s)ome had a more complicated process than others(.)" **P19** observed differences between the way tertiary apps requested additional access rights. He writes "*Some are more streamlined than others, some*

require additional info(.)" Access right may have been noticed by some participants but not necessarily seen as barriers or something worth representing. As **P16** wrote "*Logging onto third party apps via Facebook, Twitter or Google allowed for a very convenient & streamlined process without having to register for a new account. It is more convenient on the laptop than other tablets due to the interface.*"

As can be seen in **Table 63** in the Appendices, the two tasks where participants represented reaction to requested access rights more visibly is with dlvr.it and Hootsuite. Many participants felt that it was important to note that access rights had been requested as part of the tertiary authentication process. At the opposite, the access rights requested by the BlackBerry Facebook app drew less attention with a strong majority of 90% of participants. Business Organizer (80%) and Medium (75%) were also less represented by participants in diagrams.

5.3.2.4.7 Is the path linear?

I label a series of sites of interaction connected with one another and representing each control point as an interaction path. Some of these connected interactions in the participants' diagrammatic representations were not linear and branched out into parallel paths. Most participants represented their diagrams with linear paths. **Table 64** (in the Appendices) contains the results.

Most participants' mental model representations are process-based and less situational. As they performed various tasks, they did not just use an app. They used a series of small steps to achieve one goal. As expected, **P18**'s diagrams were the least linear. I expected this based on her preference for situational representation and thus less emphasis on linear paths of interaction. **Table 33** shows the detailed view of all participants' representation of linear paths of interaction, particularly **P18**'s preference for not representing them.

Table 33 - Linear Path of Interaction: Detailed View

PARTICIPANT	T3A	T4B	T5C	T8A	T9B	T10C	T13A	T14B	T15C
P01	1	1	1	0	0	1	0	1	0
P02	1	1	1	1	1	1	1	1	1
P03	1	1	1	1	1	1	1	1	1
P04	1	1	1	1	1	1	1	1	1
P05	1	1	1	1	1	1	1	1	1
P06	1	1	1	1	1	1	1	1	1
P07	1	1	1	0	1	1	1	1	1
P08	1	1	1	1	1	0	1	1	1
P09	1	1	1	1	1	1	1	1	1
P10	1	1	1	1	1	0	1	1	1
P11	1	1	1	1	1	1	1	1	1
P12	1	1	1	1	1	1	1	1	1
P13	1	1	1	1	1	1	1	1	1
P14	0	1	1	1	0	0	1	1	1
P15	1	1	1	1	1	1	1	1	1
P16	1	1	1	1	1	1	1	1	1
P17	1	1	1	1	1	1	1	1	1
P18	1	0	1	0	0	0	0	1	0
P19	1	1	1	1	1	1	1	1	0
P20	1	1	1	1	1	1	1	1	1

P01 also appears to rely less on linear paths of authentication but that is because he represented many different paths and loops that matched tertiary authentication processes happening concurrently. Unlike **P18**, **P01**'s diagrams are still process-based, as can be seen in **Figure 27** where the participant did not rely on a linear path of interaction.

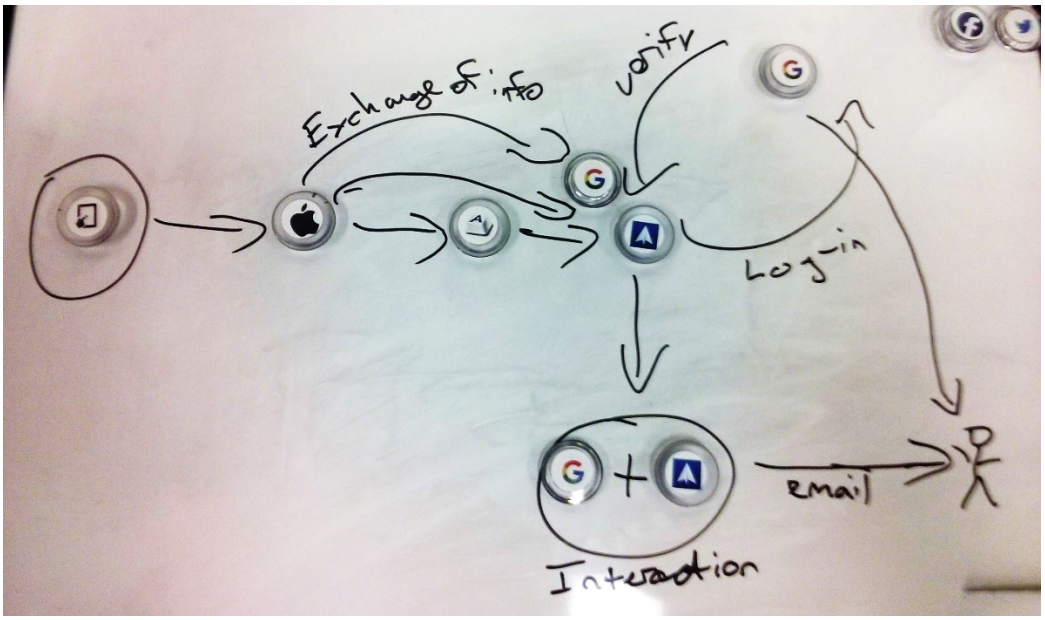

Figure 27 - P01 Nonlinear Path of Interaction Sample

5.3.2.4.8 Is the model abstract or physical?

As argued by Johnson-Laird (1983, 422), physical models represent the physical world. They often feature physical devices as sites of interactions or modalities. Abstract models represent ideas and concept. With this question, I attempt to classify which kind of mental models are represented by participants' diagrams.

To demonstrate an example of mental models classified as physical, let us observe one diagram from **P19** in **Figure 28**. This participant's diagrams were all rated as being physical by myself and the other coders who verified my coding.

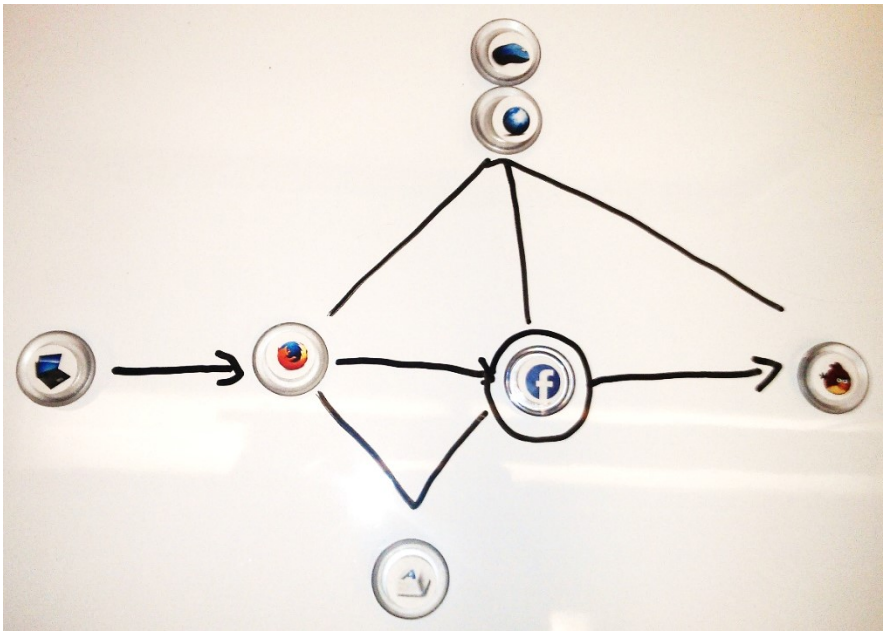

Figure 28 - Example of Physical Mental Model from P19

In the diagram above (**Figure 28**), there is a representation of a laptop that connects to the Firefox browser. From there, there is representation of a keyboard outside of the interaction path. Another branch connects to a pair of magnetic icons representing the Internet and a computer mouse. Bothe the keyboard and the pair connect to the Facebook magnetic icon. However, the pair (composed of the mouse and the Internet magnetic icons) also connects to AngryBirds Friends. Although only the laptop, the mouse, and the keyboard represent physical objects that the participant could hold, the digital sites of interaction are also physical and not

represented as ideas or concepts that the participant cannot directly interact with. A main consideration for classifying a diagram as physical was the presence of an anchoring site of interaction such as the laptop or a tablet at the onset of the interaction. Modalities of interactions such as the keyboard and the mouse added weight to physical mental model classifications.

Figure 29 is a diagram that contains an abstract mental representation from **P06**. All of the participant's diagrams were classified as abstract by myself and the other coders who verified my initial coding. The interaction represented in the diagram is the same one as that of **P19**. It is a representation of tertiary authentication using Facebook and AngryBirds Friends. In this diagram, the physical site of interaction matters less than the actions portrayed. Facebook and AngryBirds Friends are treated as concepts where interaction occurs. There are no modalities of interaction depicted nor mentions that a laptop was used as the site of interaction.

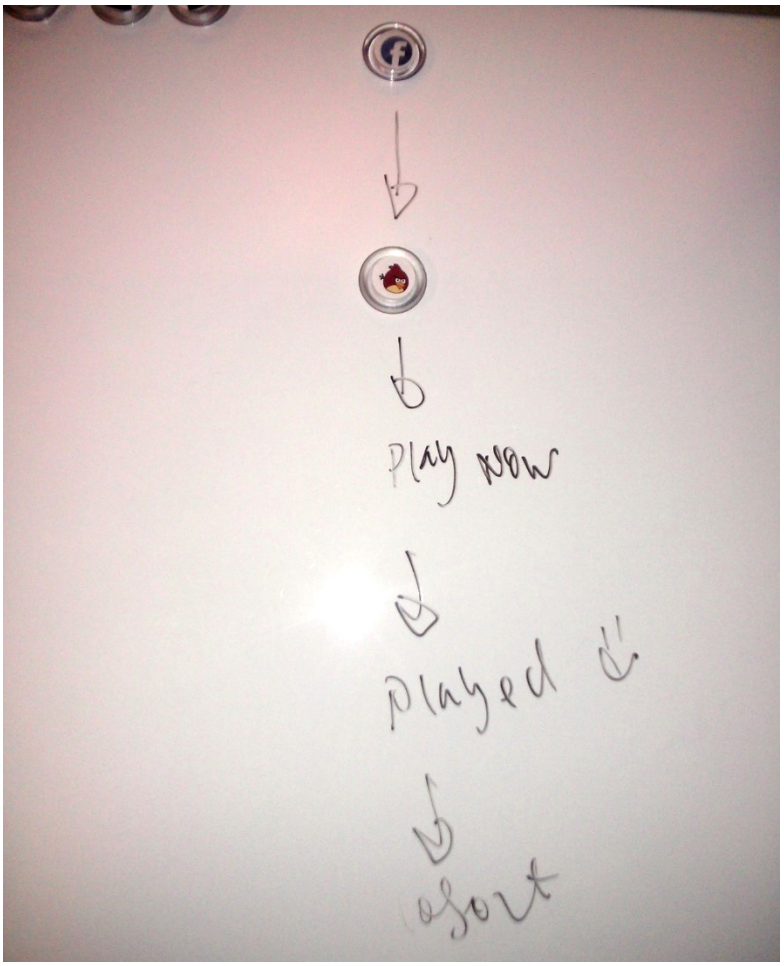

Figure 29 - Example of Abstract Mental Model from P06

Most diagrams represented physical mental models. A few integrated both abstract and physical characteristics. **Table 65** (in the Appendices) has the results.

5.3.2.4.9 Are there Pairs as Sites of Interaction?

This question asks if participants used pairs of magnetic icons and more to represent sites of interaction. During the initial evaluation of the diagram, I noticed that several participants paired magnetic icons together to represent sites of interaction. These sites may combine modalities of interaction such as a keyboard with a platform, like Facebook. Others may even pair a browser with a physical site of interaction like laptop. This data was recorded mainly to see if there were any special insight that could be gained from this diagrammatic mental model representation practice. **P16**'s diagram for tertiary authentication with Twitter in **Figure 30** is an example of pairs used in one site of interaction.

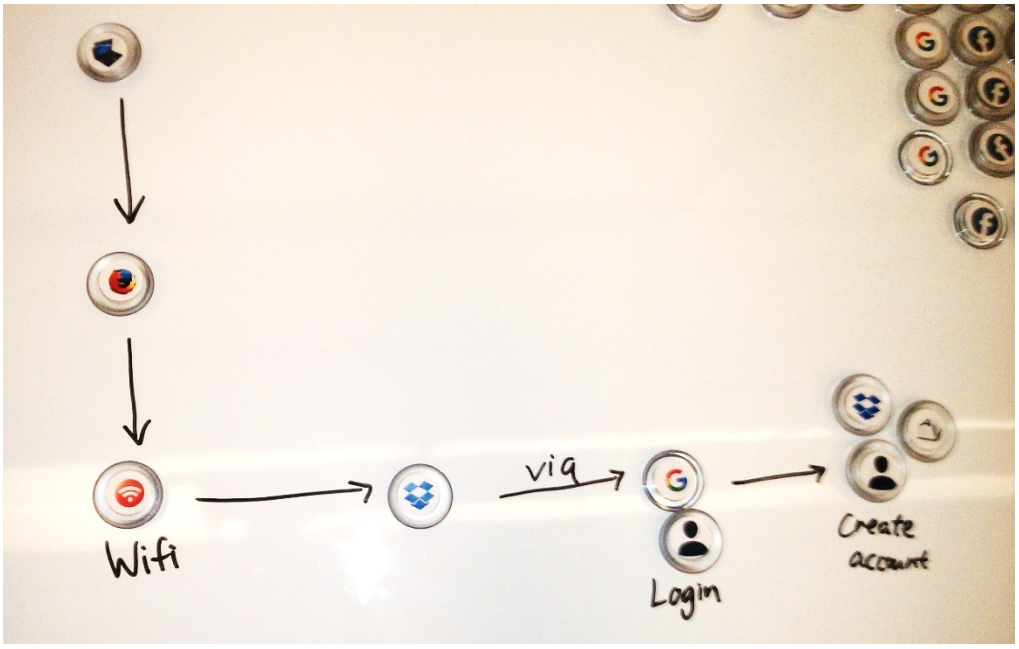

Figure 30 - P16's Paired Sample

Some participants used several magnetic icons to represent one site of interaction. These pairs may represent a typical site of interaction like the iPad, combined with a platform, like iOS. Other pairs could represent the laptop paired with a keyboard or a mouse. Most diagrams did not feature paired magnetic icons. See **Table 66** (in the Appendices) for the results.

Some participants like **P10** used the magnetic icons to represent all possibilities of interaction offered with tertiary authentication. In **P10** diagram for Hootsuite, tertiary authentication through Twitter, Facebook, Google, and direct login are represented. Twitter is the option selected as represented with the interaction path continuing in the Twitter option.

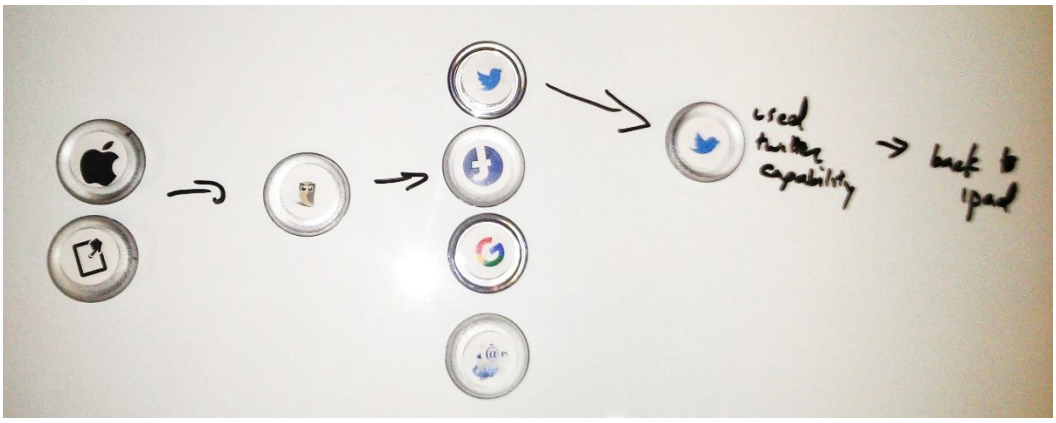

Figure 31 - P10's Paired Sample

5.3.2.4.10 Does the primary platform precede the tertiary authentication?

This question was added because several participants listed in their diagrammatic representations that the primary platforms were accessed before the tertiary apps and services. For many, authentication into a primary platform occurred before they encountered the tertiary app as seen in **Figure 32**.

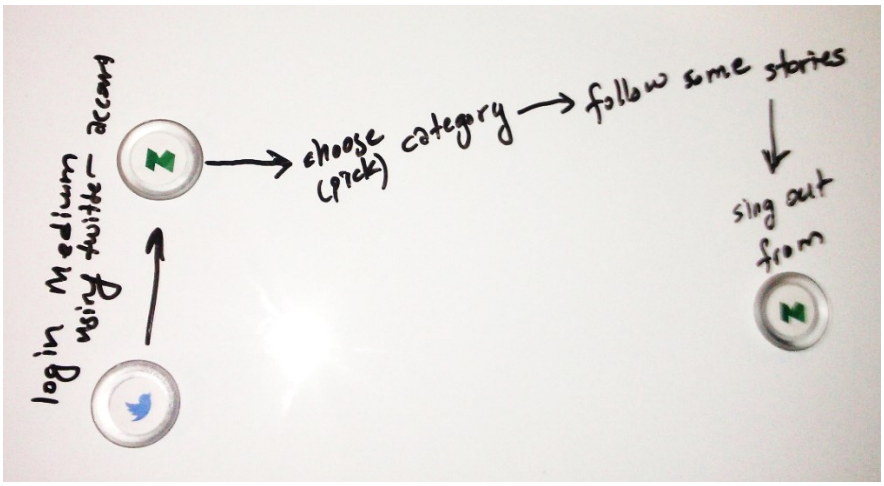

Figure 32 – P02 Primary Before Tertiary

This was an interesting finding as in each task, participants were handed the laptop or the tablets with the tertiary app or services already loaded with the primary platform is part of the tertiary authentication process. So, when I indicate that the primary platform precedes the tertiary authentication, it is important to understand that it is a part of a whole. Similarly, the tertiary app can be said to precede the tertiary authentication if it precedes the primary platform. The tertiary authentication is a process made of both a primary platform and a tertiary app. While most participants' diagrams did not represent the primary platform before the tertiary authentication, the results in **Table 67** (in the Appendices) were significantly different with AngryBirds Friends and with the BlackBerry Facebook app. For AngryBirds, participants landed on Facebook first and had to log to see the AngryBirds Friends game. For the BlackBerry Facebook app, no single magnetic icon represented the app. Participants used the regular Facebook magnetic icon to represent the BlackBerry app and tertiary authentication.

5.3.2.4.11 Is the tertiary authentication part of the interaction path?

For some participants, the tertiary authentication was not included as part of the interaction path. It was a process that occurred outside in a loop or parallel branch. To effectively classify a tertiary authentication as being outside of the interaction path there must be a relationship between a primary platform and a tertiary app. It can be a process happening in a loop outside of the interaction path. However, while it appears as a logical prerequisite for a relationship[16] between a primary platform and a tertiary app to exist, there are some cases where there were no indications of tertiary authentication at all. Diagrams where there were no tertiary authentications represented were still coded as having no activity on the interaction path. For an existing tertiary authentication to be coded as outside of the interaction path, the primary platform was the component that had to be outside of the path. Tertiary authentication only happens when there is a relationship and between a primary platform and a tertiary app. **Figure 33** from **P01** illustrates how primary platforms could be outside of interaction paths, when they did occur.

[16] By relationship between primary platform and tertiary app refer to the thematic question above for what constitutes a definition.

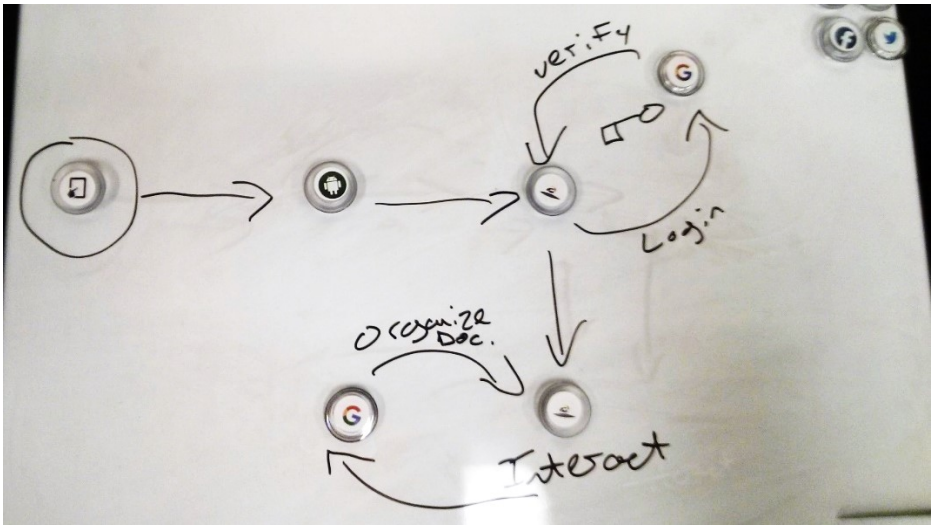

Figure 33 - Tertiary Authentication Outside the Interaction Path (P01)

While most participants chose to represent the tertiary authentication as part of the interaction path, several represented that process as happening outside, often in a loop exchanging information between the tertiary app and the primary platform. The only exception, as seen in **Table 68** (in the Appendices) was with the Playbook where a clear tertiary authentication process was difficult for most participants to represent.

P09 is the only participant to have represented tertiary authentication with the Blackberry Facebook app for the Playbook. The coders and I chose to classify this as a tertiary authentication because of the errors that **P09** had to rectify in his Facebook account to allow the tertiary Facebook app by Blackberry to have access to his personal account. This demonstrated a clear understanding that the Facebook platform and the Facebook Blackberry app were separate entities, as seen in **Figure 34**.

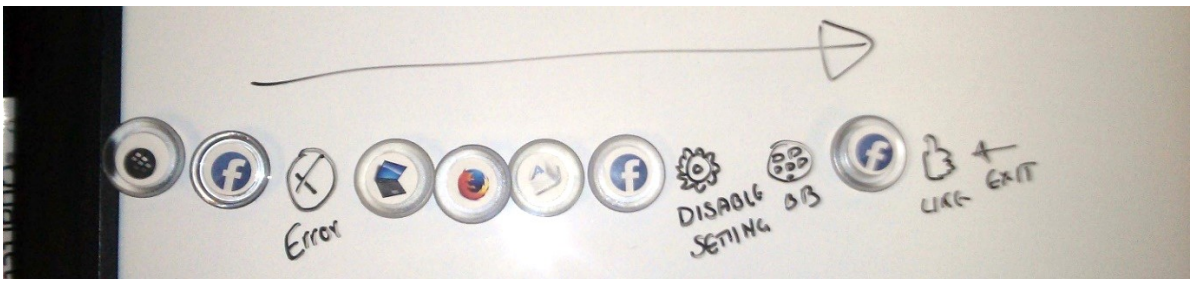

Figure 34 - Facebook for Playbook Tertiary Authentication (P09)

5.3.2.4.12 Is there a Differentiation?

The differentiation of the operating system from the device, or an indication that there is a separate site of interaction between a device and a browser, or the Internet itself indicates that participants understand that the device has a physical layer, and logical ones. Thus, it demonstrates a level of technological literacy and adheres to Clark's (2012) control point analysis framework which is at the core of this study.

Differentiation also helps us understand people's perceptions of security, confidentiality, and privacy as the affordances of each site of interaction can affect how participants perceive risks. For example, **P19** indicated awareness of differentiation when responding to security concerns about tertiary authentication. He writes about his concerns that "*[his] data would be copied to different devices.*" **P20** adds "*Sometimes I feel unsecure opening my accounts in public devices(.)*"

I compared the differentiation between the operating system and the device (mobile); the browser from the laptop; and indication of an independent Internet for both tablets and the laptop. Differentiation occurred more often when participants represented interactions with mobile devices. As seen in **Table 69** (in the Appendices), except for the Playbook where results are evenly spread, all other mobile devices represented the operating system and or the browser.

5.3.2.4.13 Where is the initial site of interaction?

This question asks about where the participant first represented where their session started as they performed each task in the quasi-experiment. The tablet (for mobile-based tasks) and the laptop (for laptop-based tasks) were respectively represented the most as the initial sites of interaction. **Table 70** (in the Appendices) includes the results.

5.3.2.4.14 Where is the last site of interaction?

This question asks about where the participant represented where their session ended as they performed each task in the quasi-experiment. The last site of interaction often had to be inferred as it could be a submenu part of an app. Modalities of interactions cannot be sites of interaction so which site they affected had to be inferred. The results for this task in **Table 71** are

the most interesting. There are no overall patterns. The frequencies should be understood per task. Most participants represented tertiary apps as the last site of interaction when they were tertiary services and standalone products such as AngryBirds Friends (75%), Medium (75%), and Dropbox (60%). Other results varied.

5.4 Conclusion

While conjectures 2 (how users rate the value of their profile when told that the cannot edit or remove data shared with third parties during tertiary authentication) and 3 (users will selectively restrict access to their profiles when they have the option when being knowledgeable about what is shared during tertiary authentication) proved null, a pattern can be observed about how participants prefer to interact with privacy policies and usage terms. It appears that they are more inclined to adjust their privacy and security settings than reading policies about those topics.

In the next chapter, I perform a policy analysis of the security and confidentiality policies at Facebook, Google, and Twitter using four approaches. They are;

a) Technical analysis of OAuth authentication process;
b) A perceptual evaluation based on Dourish's (2001) embodied interaction;
c) A policy analysis using frame analysis, and;
d) An analysis using the transactional token theoretical framework introduced in this dissertation.

Chapter 6
Findings – Policy Analysis

The policy analysis is an evaluation of the confidentiality and security policies and practices at Facebook, Google, and Twitter to understand how they seek to protect users' profiles, protect themselves from legal liabilities, enhance the usability of the platforms, and implement tertiary authentications with third-parties. The policy analysis is the first step needed to answer my **RQ1** which asks to what extent of the interplay between security and usability in the commodification of users' personal data during tertiary authentication. The policy analysis when combined with Conjecture 1 will allow me to answer **RQ1**.

6.1 Introduction

The policy analysis that I perform also sheds some insights about the two other research questions of this dissertation. My second research question investigates how are people managing and controlling their security and confidentiality as they perform tertiary authentications. From this research question, two subsequent conjectures follow.

C2 measures user control and management of personal information during tertiary authentication. In the theoretical framework chapter, I outlined the processes involved in personal information sharing between people, platforms, and third parties. I called this process the transactional token. The policy analysis allows me to identify what personal information is shared between primary platforms and tertiary clients. It also explains how this process works technically. To this end, I investigate the mechanics employed by Facebook, Google, and Twitter to exchange people's personal information through tertiary authentication.

C3 measures how users rate the security of their personal information when aware that it is not editable or removable while performing tertiary authentication and shared with third-parties.In the quasi-experiment that I performed to test this conjecture, the test group's participants were informed of this by reading the privacy, security, and data policies of Facebook, Google, and Twitter. The policy analysis that I perform investigates the contents of these documents.

RQ3 asks which conditions and variables create a perception of false security in users performing tertiary authentications. It seeks to uncover the factors of tertiary authentication that affect users' sense of security. This research question is partly answered through the quasi-experiment that tests **C1**. This conjecture, as I hinted in the beginning of this chapter, theorizes that people's mental models about tertiary authentication differ from the platform operators' design models.

The policy analysis allows me to document and set the design models used by Facebook, Google, and Twitter for their tertiary authentication. Having identified the design models of the platform operators, I will be able to use them in a comparison to the mental models of the participants in my study. This comparison is presented in the results chapter of the dissertation, below.

In the literature review chapter, I defined design models as representations of how things work from the perspective of the instigator of a technology, or in the context of this study, a platform operator. The design model differs from the mental model of a technology user. Mental models, as argued by Norman (2013), are representations from the perspective of a person of how things work.

I supplement my evaluation and reconstitution of Facebook, Google, and Twitter's security and privacy design models with an analysis of their data, security and privacy policies. As suggested by Fuchs, these public documents can be perceived as biased and meant to protect companies with legal jargon, often hard to decipher by the public, and demonstrate to legislators a capacity to self-regulate (2014, 165-166). Yet these documents are still the ones that users, such as some of the participants of this study, are exposed to as they performed their tertiary authentication with platforms.

My policy analysis uses the transactional token framework presented in the theoretical chapter to code and interpret the documents but also relies on other analytical methods such as control point analysis and discourse analysis. Before starting the policy analysis, I will review similar analyses from the literature on social media, information systems, and authentication.

6.2 Related Work

Privacy policy reviews is an active area of investigation within the broader field of information policy research. Concurrently, the past few years have seen an increased interest within the field of HCI research, and particularly in areas such as usable privacy, on improving users' interaction with systems that involve private data. At the same time, we are witnessing a proliferation of systems, apps, and platforms that depend on users' private data for their commercial success. As such, the two previously-unrelated fields of information policy and HCI are increasingly overlapping. I review here recent research efforts within this growing space. Each part offers opportunities for an exhaustive evaluation of platform operators' design models because of the gaps that they do not cover.

6.2.1 Privacy Policies

Most of the privacy, data, and security policy research focuses on Facebook. Often, studies related to privacy policies address this topic as an ancillary concern to privacy and users. In 2012, Wilson et al. (2012) reviewed and listed 75 scholarly studies alone. While they detected an increase in user concerns for privacy on Facebook, they did notice the tension that Facebook faced in encouraging increased personal information sharing while maintaining weak security and access controls (Wilson, Gosling and Graham 2012).

Anja Bechmann (2014) presents original research on Facebook users and informed consent measures taken to inform participants in a Danish study. She argues that users' acceptance of privacy policies must be understood as a group-based practice where they perceive benefits from adhering to Facebook and accepting the sharing of their personal information (Bechmann 2014). Bechmann observes that there is a trade-off between the actual places in Facebook where users share information (2014). Some, like the timeline is considered public whereas messaging and emails through Facebook are considered private (Bechmann 2014). Bechmann's study points to the diverging conceptual models between Facebook and its users. Facebook gathers data about its users at every point of interaction, regardless of whether the people perceive the space to be public or private.

Anna Johnston and Stephen Wilson (2012) observe how Facebook's data collection policy and practices contradict the precepts suggested by Australia's Privacy Act of 1988 which is inspired by the Organization for Economic Cooperation and Development (OECD) like that of many other jurisdictions. The 1980 OECD Council guidelines suggest that data collection from individuals performed by groups, legal persons and other entities should be limited to what is needed (OECD Council 1980). Johnston and Wilson note that Facebook routinely collect personal information from users that is unnecessary for its platform to function (2012).

Laura Stein (2013) explores the level of user participation in the design of platform policies. Of the three platforms that she reviews, which includes Facebook and YouTube, she finds that Wikipedia is the only one where people can influence the terms and conditions of their usage due to its participatory nature and shared governance (Stein 2013). She argues that as well as describing the power relationships between platforms and individuals that policies also describe the power relationships and responsibilities of platforms and polities (Stein 2013).

Yang et al. (2015) performed an experiment on users' cognitive processes as they encountered privacy policies on websites sporting privacy seals. In their findings, the researchers observed that familiarity with a website caused users in their study to perform less verification of privacy policies (Yang, Ng and Vishwanath 2015). Sites with privacy seals, whether they were familiar or not had even less users reading their policies (Yang, Ng and Vishwanath 2015).

Gerber et al. (2015) conducted an evaluation of the Android permission system Google enacted in 2014. They observed that while Google was attempting to simplify the permission system when users installed third-party apps, that they created more risks for users through the confusing and barely visible update app system which did not list prominently new access requests from third parties. This research is interesting in that access permission systems are analogous to privacy, data, and security policies in mobile interaction.

G.S. Hans (2013) criticizes the inadequacies of the American Federal Trade Commission (FTC) regulations in dealing with unfair privacy practices with Facebook, Google, and Twitter. He argues for changes to the FTC's regulation to better protect American consumers (Hans

2013). In his study, Hans provides a detailed legal history of the three platforms' judicial and regulatory dealings with the FTC.

Building from the practice of using privacy policy goals as components to enable information systems' design, Bhatia et al. (Bhatia, Breaux and Schaub 2016) propose a framework to extract goals using crowdsourced reviews and natural language processing. While they propose a method to operationalize goals expressed in the texts of the privacy policies, their approach is best for new platforms and iterative development. It does not consider the context and the constraints of the privacy policies on users.

Cranor et al. (2006) developed a third-party platform called Privacy Bird to advise users of the contents of privacy policies. This system was developed to mitigate the complexity of privacy policies as people encountered them. There is a parallel to Cranor et al., other Platform for Privacy Preferences (P3P), and the framework proposed by Bhatia et al. These proposals immerse themselves between the user, the developer, and the privacy policies to interpret and make sense of the latter. However, these proposals create another layer of interaction instead of understanding the context in which the privacy policy is deployed to the public who is expected to interact with a policy document. My perceptual evaluation centers on the practices of platform operators as the site of interaction that must be understood to design usable privacy policies.

McEwen and Scheaffer (2013) investigated the practices of Facebook users following the death of a friend, colleague, or family member. In their study, they found that at the time, Facebook used privacy as the main thrust of some of its policies concerning the control of deceased members' accounts (McEwen and Scheaffer 2013). McEwen and Scheaffer note that in 2013, Facebook argued that to protect the privacy of the deceased, login information to their accounts was limited (2013). Friends could continue posting to the deceased' profile based on the former's privacy settings (McEwen and Scheaffer 2013). While McEwen and Scheaffer analyzed Facebook privacy policies and terms of use, their investigation was not focused on how users perceived, interacted, or even reacted to these policies. Although participants did react to the enforcement of specific policies by Facebook as was the case when Facebook removed recently memorialized accounts from the victims of the Virginia Tech shootings (McEwen and Scheaffer 2013).

The privacy policy studies mentioned above do not approach audience commodification from an interaction perspective. For example, privacy policies may codify the practices of platform operators but they do not circumscribe their values and corporate cultures. These values and cultures are not addressed directly by the literature below. For example, when Fuchs (2012,b; 2014) reviews privacy policies and third parties, he ignores actual practices and the context developers producing third-party services operate in.

6.2.2 Developers' Policies

Research about primary platforms and tertiary developers is sparse. Much of the literature available is in the form of training materials for developers (Boyd 2012; Martinelli, Topol and Nash 2015; LeBlanc and Messerschmidt 2016) produced by technology publishers like O'Reilly. In a topology of research on Twitter, Michael Zimmer and Nicholas John Proferes (2014) criticized the lack of ethical concern in research about Twitter data and collection by scholars who perceived any Twitter data stemming from its API as being public by default.

Erik Borra and Bernhard Rieder (2014) contributed a programmed software framework to collect data directly from Twitter's public APIs. They discuss the efficacy and problems related with other methods of data collection and address some of the ethical and technical problems encountered while working with Twitter's data (Borra and Rieder 2014). Their research focuses on technical processes that researchers can replicate for research as opposed to the tools and methods used and available for common developers.

Yet Bergvall-Kåreborn and Howcroft (2013) offer a rare study in the labour practices of third-party developers producing apps for Apple's iOS and Google's Android mobile platforms. Their study demonstrated that many independent developers worked in precarious conditions rife with competition, with limited control over the commercialization of their products and fear of obsolete skills, and obsolete products for obsolete platforms. Instead of the high-level knowledge entrepreneur, their study depicts a professional space where information technology workers reproduced traditional corporate labour processes (Bergvall-Kåreborn and Howcroft 2013). Bergvall-Kåreborn and Howcroft discuss the power imbalance between third-party developers and platform operators Apple and Google (2013).

In another study Bergvall-Kåreborn and Howcroft (2014) discussed the business practices of third-party developers producing apps for iOS and Android. Here, they directly addressed some issues related to business strategy and the documentation practices of platform operators (Bergvall-Kåreborn and Howcroft 2014). While their study continues to describe the relationship between platform operators and third-parties as asymmetrical and precarious for the latter, they also borrow from Zittrain's closed and open system framework to explain the mobile app development and distribution (Bergvall-Kåreborn and Howcroft 2014).

In the literature reviewed, there is little mention of the coded language within developers' documentation. Yet platform operators need to maximize the opportunities of third-party developers with their audiences as they benefit both parties. The values coded into these platforms must reflect a win-win approach to entice third-party developers to produce apps and services for the primary platform. As Bergvall-Kåreborn and Howcroft remarked, platforms are competitive with one another and to attract more users (2014). They must invariably be able to attract and retain the most developers.

6.3 Approaches and Method

This policy analysis was an evaluation of the privacy policies and practices at Facebook, Google, and Twitter to understand their design models that they rely upon to allow users to perform tertiary authentications. As I argued in the literature review, design models explain how platform operators, designers, and developers think the products and service they design, work. Design models stand apart from mental models which represent how people think things work.

The policy analysis did not involve any participants. It was used to ground the empirical data collected in the study. Documents were obtained through the public domain. No formal interviews with operators at Facebook, Google or Twitter were planned nor conducted.

I performed four analyses. First was an analysis and review of the technical processes involved in tertiary authentication. Next, I performed a perceptual evaluation of how the platform's design shape how users interacted with them. The platforms are sites of interaction that allow people to perform some acts or constrain them. The first act is usually the registration process which involves the discovery of the privacy and other policies by users.

The next analysis that I performed was a frame analysis of some of the privacy and security policies that people must agree to when using Facebook, Google, and Twitter. Each company's policies differ in approach. Frame analysis is a way to understand the narrative behind the documents presented to users. I collected similar policies from Facebook, Google, and Twitter which were also used in the quasi-experiment with participants, as described previously. I collected other documents from the platforms operators, such as developers' policies, and a white paper on personal data commissioned by Facebook for the frame analysis.

For the Facebook analysis, I used the data policy released on January 29, 1026 (2016). For the Google analysis, I used the privacy policy released on August 29, 2016 (Google 2016). For the Twitter analysis I used the privacy policy released on September 30, 2016 (Twitter 2016).

Finally, I used the transactional token framework introduced in the theoretical chapter to perform the last evaluation of the platforms' practices with users performing tertiary authentication. While there is no dedicated control point analysis of user interaction with tertiary authentication in the policy analysis, this method introduced by Clark (2012) influenced both the transactional token framework and the perceptual analysis.

The goal of these policy analyses was to help me explore my theoretical concept of the transactional token and determine the validity of this conceptual construct. The policy analyses also helped me construct the broad research design of the user studies research that I performed in the human-computer interaction part of my study.

6.4 Technical Background & Analysis

How tertiary authentication has developed offers an interesting insight into how people shape and interact with technologies beyond their original scope. Tertiary authentication is a solution to distributed computing that was developed to streamline the number of profiles and accounts people had. Tertiary authentication provides users and platforms single-sign-on utility (SSO).

Originally SSO utilities like Security Assertion Markup Language (SAML) launched in 2002, offered large enterprise management resources to manage the labour of their employees across several points of interaction while responding to the classic usable security dilemma pitting security versus usability (Reimer, Abraham and Tan 2013). Information workers in large enterprises needed to perform authentication in many platforms from different vendors at once (Lockhart 2005).

For example, a professional stock trader may use Bloomberg Terminal and Moody's Analytics in his everyday practice. A SSO could allow him to interact and authenticate within several platforms with one user account. It could also allow his employer to manage, lock, or terminate these accounts should the employee move to a competitor (OneLogin 2015). SSO systems provide managers an opportunity to control the labour of their employee (Zuboff 1984).

SSO is a way for information systems to allow users to use the same authentication. An independent federated process manages the user's account and allows it to be shared between multiple platforms. One of the most popular SSO processes before 2007 was OpenID. Released in 2005, OpenID proposed to increase the usability of users' information practices by allowing them to use one profile to authenticate themselves in several Web-based venues.

By 2007, OpenID's most recent versions came short of answering the needs of large platform developers who wanted to add authentication capabilities for native platforms beyond browser-based venues such as websites (OpenID 2017). The relaying resources exchanging user account data worked best within browsers (OpenID 2017). The exchange format, Extensible Markup Language (XML) also proved difficult to work with (OpenID 2017). OpenID was ill-suited for mobile apps needing to authenticate users in native apps (OpenID 2017). Ubiquitous computing and changes in people's embodied interaction encouraged developers to seek alternatives suited to mobile usage.

OAuth is an alternative solution to enable tertiary authorization developed in 2007 by Twitter developers aggregating standards and practices from different platforms from Google, America Online (AOL), Yahoo, and Flicker (Hammer-Lahav 2007). Instead of sharing protected resources between two sites of interaction, platform operators found OAuth a suitable alternative

to allow users to perform authentication on mobile platforms without relying on browser architectures (Chen, et al. 2014).

Authorization differs from authentication. Authorization in software development allows one platform, known as a customer to use protected resources from another platform (Chen, et al. 2014). A benign example would be a system designed to share protected fonts between a platform and third-party websites. Here, the third-party developers can use the fonts without having access to the password (authentication) of the platform's server.

OAuth 1.0 which was taken over by the Internet Engineering Task Force (IETF), the Internet governance body for technical standards, allowed developers to enable users to use their accounts with other services without revealing their passwords to the third-party with whom people were interacting (Parecki 2016, a). OAuth 1.0 worked by allowing a client server (the third-party) to request that a user grant permission for a token obtained by the service provider (the primary platform) (Internet Engineering Task Force 2010). The token was used in lieu of a password and a user name with the third-party server (Internet Engineering Task Force 2010).

Platform operators from Facebook, Google, Twitter and others found that the authorization utilities of OAuth could be used to exchange user tokens instead of protected resources, such as images, specific processes, like APIs, sounds, or fonts. OAuth was not developed to exchange user logins. However, developers found OAuth 1.0 and its update OAuth 1.0a which corrected security flaws, wanting (Parecki 2012).

Tokens could be obtained through three specific flows. Flows, which are different sites of interaction, allowing client servers to obtain flows for web-based, desktop applications, and mobile devices (Hammer-Lahav 2010). These proved insufficient for developers who felt that forcing users to open web browsers while in native apps to authenticate tokens was poor user experience (Hammer-Lahav 2010).

OAuth 2.0 is a complete redesign of the standard that address developer's complaints with OAuth 1.0 and 1.0a. One of the main changes was the abandonment of cryptographic token requests which developers found difficult to develop (Hammer-Lahav 2010). Authentication is

now contained within a bearer token like a web cookie that is sent through secured HTTPS protocol (Internet Engineering Task Force 2010).

An important addition in the redesign of the three existing flows into six new ones for OAuth 2.0 was the dedicated password and username flow (Hammer-Lahav 2010). This added indirect authentication as tokens that could be exchanged between information systems (Parecki 2016, b). User accounts held with one primary platform could now be exchanged like any other commodity, such as images, sounds, or fonts with tertiary apps or services.

OAuth 2.0 has become the dominant tertiary authentication process (Cherrueau, et al. 2014). Although they each use other mechanisms for some specific operations, Facebook and Google both rely on OAuth 2.0 to enable tertiary authentication. Twitter still uses OAuth 1.0a for tertiary requests that seek to authorize clients to act on behalf of users (Twitter 2017). For example, if a user wants to allow a Twitter client to post tweets on her behalf, OAuth 1.0 is used. Twitter offers limited support for OAuth 2.0 for other operations (Gerlinger 2013).

Each version of OAuth has security flaws that can be exploited if the transmission of tokens is compromised (Paul 2010; Gibbons, O'Raw and Curran 2014). Yet OAuth deployment is at the core of the tertiary authentication practices of Facebook, Google, Twitter, and many other technology platform operators. The rationale for using OAuth is based on the convenience and utility to platform operators. It is not based on the need to secure users' interactions with platforms.

The original rational was based on the needs of enterprises to better manage the work of their employees. There are many parallels to the deployment of SSO towards the public and the transition from shared computing that I described in the Literature Review Chapter. The same way that shared computing which was based on the needs of enterprise gave way to personal computing, mobile and ubiquitous computing made SSO a relevant form of human-computer interaction beyond the realm of the enterprise.

6.5 Perceptual Evaluations of Policies

Privacy policies, often the first documents people interact with when using sites and apps, inform users about how data about them is used and collected (Cranor 2005, 448). Yet users' understanding and interactions with these documents are often problematic (Jensen and Potts 2004). To users, they may appear complex, are often skipped, or just agreed upon without a careful read through (Milne and Culnan 2004).

Research dedicated to understanding users' interaction with privacy policies have focused on their contents (Grossklags and Good 2007), users' mental models (Coopamootoo and Groß 2014), and their perceptions (Adams and Sasse 1999). While these user-centered approaches have yielded results, I propose an alternative perspective focused on the evaluation of platform operators' design models of user interaction with privacy and security policies. Instead of simply reviewing the texts of these policies, I propose an approach inspired by Paul Dourish's (2001) embodied interaction theory.

My perceptual evaluation offers us a glimpse into how privacy policies can affect users but instead of investigating their contents, we want to understand how they are designed for user interaction. User privacy policy analyses often look at how users perceive, and read documents (Jensen and Potts 2004), their strategies for dealing with privacy concerns and how they set their personal settings to mitigate risks (Johnson, Egelman and Bellovin 2012). This approach yields results but does not focus on the context where users interact with platforms. Users also have opportunities to interact with privacy policies, especially when they create new accounts on platforms. Often, as they register an account for a platform, people must consent to the contents of a privacy policy or related terms of usages documents. This is where perceptual evaluations of privacy policies become the most relevant. Such evaluations allow researchers to map and understand what happens after the user has skipped to the bottom of the agreement or ignored a prompt to open a separate link to become aware of the policy's contents and how their information is collected by platforms.

In this section, I performed a perceptive evaluation of the privacy policies designed by Facebook, Google, and Twitter as they are presented to end-users interacting with the platforms.

Specifically, we observe how users are introduced to the privacy policies as they register for new accounts on the platforms. Registration is one of the most important moments where users interact with privacy policies. The other site of interaction with privacy policies is where users adjust their privacy settings. The privacy settings are developed from the privacy policies.

6.5.1 Facebook

The original object of verification to access Facebook upon its launch in 2004 was the university email address. Access to the platform was once limited to Harvard University students and then a few Ivy league American colleges (Brügger 2015). Gradually, more university students were able to join Facebook where they could recreate and expand their networks (Brügger 2015). As dramatically represented in David Fincher's film *The Social Network* (2010), early Facebook users' personal information was easily accessed by Facebook founder Mark Zuckerberg who was everyone's first friend. This first friend was still a third-party for most early Facebook users.

Facebook relied on gamification early on to "hook" its users to its platform. In this research, I borrow the gamification definition of HCI scholars Cathie Marache-Francisco and Éric Brangier (2015). Their definition of gamification focuses on sensory-motor-based interactions, user emotional engagement, and cognitive goal resolutions (Marache-Francisco and Brangier 2015). Gamification integrates game practices and designs into non-game-based information systems (Rapp 2015).

Users had to perform game-like interactions and operations as they decided who was a friend, added them, poked them and exchanged with them. This was like a game to collect the most points, except here users collected the largest network of friends as if they were tokens and points that could add value to their own account and social standing.

The value of Facebook was the network, so, when it allowed access to its platform to non-students, verification was no longer obtained through a university email, but one that allowed Facebook to reconstruct a network of users based on the contacts associated with this address. Today, when registering a new Facebook account, the first action that Facebook urges new users to do, is to enter their email addresses so that its internal network search engine can

find other users who may be part of this network. The email address as well as being an important means of registration and verification becomes the means by which access to the Facebook network will be determined for the new user.

The second action that Facebook suggests of its new user is to take a privacy tour. The user was never asked to agree formally to a contract or terms of use of the 2016 data policy (Facebook 2016). She was never told about Facebook's privacy demands. Instead, she is invited to adjust how she controls her confidentiality on the platform with a series of widgets and tools that she must play with. Only later if she finds the time and the will, will the new user be confronted with the fact that by enrolling into Facebook (2016), terms of privacy and security were assigned to her without her ever agreeing other than by entering an email address and adding her name.

The third action that Facebook requests from new users is to reveal more personal information about themselves than their names. Facebook urges new users to upload a picture of themselves. It even offers an option to take this picture from the webcam of the user's device, if a picture cannot be uploaded. Fairly quickly, Facebook attempts to put a name, an address, a face, and a network on the new user.

Before full access is granted, the new Facebook user must perform a verification from an automated email sent by the platform. Without this response, access will be limited as the user's verification will be in doubt. This action is not listed sequentially in the original timeline of the platform but now appears at the top of the browser as a constant reminder that access is conditional of the user's verification.

In 2007, Facebook introduced Beacon, a means to track its users' interaction across participating third-party websites (Brügger 2015). Every time a user shared a link of a page from a third-party website in their timeline, the host of site was notified (Brügger 2015). Beacon was criticized by privacy-minded members and of civil society organizations in the United States and abandoned by Facebook (Kuehn 2013). In reaction, the company's privacy practices were investigated by the Privacy Commissioner of Canada for in 2009 following a complaint by members of the Canadian Internet Policy and Public Interest Clinic (CIPPIC) (Denham 2009)

about a possible non-compliance of Canada's *The Personal Information Protection and Electronic Documents Act* (PIPEDA) (Minister of Justice 2015). The resolutions resulting from the complaints with the Privacy Commissioner of Canada and a settlement with the FTC in the United States, in 2012, for privacy violations encouraged Facebook to modify its privacy policy and the way users interact with it (Hans 2013).

Facebook spells out its need for user data while setting parameters in permissive modes allowing people's personal information to move easily within the platform (2016). It is up to users to remain vigilant and to continue to adjust settings which are frequently changed unilaterally by Facebook. This results in a cat and mouse game where users must react to Facebook's prompts and ever-changing settings. Users cannot set their privacy and security settings once and forget about them. If they want to maintain some control over their personal information, they must take play Facebook's monetization game.

Over time, as the user has been using the platform, Facebook will continue to post prompts at the top of the screen where it will gradually ask her to share more personal information with the platform. Information can include, occupation, marital and relationship statuses, age, religion, location, and a phone number (Facebook 2016). New data policies have been released as top screen prompts too, but they differ from the gamified way Facebook presents its privacy and security features.

Facebook's 2016 privacy policy is no longer authored as a contract that users must agree with before they can register and access the platform (2016). Instead, it is either a long document, with a series of presentations, some of which include videos or dedicated sites where privacy and security are handled from a control panel. The control panel, referred to as 'Settings' is where the user must decide the extent of the personal information that he posts on Facebook will be shared with his friends, his friends' network, and the public at large.

The interaction with the settings is a game where the user decides how much others can know about him through Facebook. While some options are locked or limited by Facebook's need to share basic information about users to sustain the viability and a functioning network, the

user can even create categories of friends with who he will share information. He can also block some users completely.

While this gamified interaction with privacy and security control panels occurs, none of the settings allow the personal information already held in confidence by Facebook to be permanently removed, forgotten, or not shared with the third-party app developers and advertisers who rely on this data from the company as part of their business ventures.

Options to permanently shut an account exist yet Facebook imposes a delay as to when the data of a user will be permanently removed (Facebook Help Center 2017). Facebook also offers unclear instructions as to how a user can permanently pull away data held by a third-party. Confidentiality is obscured by Facebook in exchange of a complicated and gamified control panel where users are encouraged to adjust their sharing parameters with their network but also with advertisers.

Facebook is vague about the interaction metrics that it uses to collect data from users (2016). Users have no options to compel Facebook to permanently delete any of this data or prevent the platform from collecting more. Facebook presents collected user data about what people have added or clicked on the platform. It does not include data obtained from the tracking of user interactions where there was no input of semantic information or a reaction to a button, or a link.

For example, Facebook does not share with users data about how long a session usually lasts; at what time they usually log in; from what location they are known to use the platform; who according to Facebook has the strongest links to individual users; what kind of news, images or posts Facebook determines as being favoured by users. Yet behavioural metrics may be Facebook's best source of knowledge about its users.

I contend that Facebook's privacy features have been optimized to respond to complaints from civil society and government institutions through gamification. Users are given clear control panels to adjust their privacy features, yet this does not curb the personal data collected from users nor does it offer any form of security from third-parties who operate through Facebook's platform. Facebook's privacy features are sandwiched in the middle of two services

that maximize the networks primary need for personal data. New users are prompted to generate a network through their emails and to add personal photos of themselves.

Before being able to use more services, users are not prompted to agree to a confidentiality policy. They are not even aware of such contract between themselves and Facebook. Instead, they are prompted to confirm their identities by responding to a verification sent to their email address.

6.5.2 Google

Starting as a free public service Google did not originally promote user authentication through its own proprietary means, such as the Gmail email account. The first non-enterprise[17] users who required dedicated user accounts to interact with Google were those who paid to use Google AdWords and those who were paid to publish Google AdSense ads. Unlike Facebook, Google's first users were advertisers and publishers. They were not common users or even university students from Ivy League schools.

Google services and apps geared for the public that had to be accessed with a Google-sponsored account started just after the company introduced the exclusive Gmail account in 2004 Gmail email addresses were at first offered to selected individuals that had relationships with Google (Robison 2008). However, the Gmail account did not become the main site of interaction for users attempting to authenticate and use various Google services until 2011 with the launch of the Google+ account.

Google made its Gmail account desirable by offering larger amount of data than competitors such as Microsoft's Hotmail (Google 2004) and by limiting who could get an address by exclusive invitations and recommendations (McCracken 2014). Only later did Google expand access to its prized email address to the public. Scarcity was also used as a strategy to create a demand for Google+.

[17] Outside of Google Search servers services for enterprise clients.

While Google+ accounts were pushed by Google to set this account as the site of interaction with its services and apps, to this day, users can still log in with alternate email accounts. Unlike Facebook, Google launched several products and integrated many services and apps with their own independent authentication systems, such as YouTube. Facebook also purchases companies, but it does not launch separate services using alternative authentication.

The number of differing services and apps hosted under Google encouraged the company in 2012 to attempt to reconcile all its privacy and security policies under a privacy policy and a single term of usage policy (Whitten 2012). This effort was the culmination of the various elements of the platform that had attempted to merge and reuse Gmail-based authentication in the past. For example, Gmail became the site of interaction and authentication for every Android user using a mobile device with this operating system. Google+ and the single usage policies of 2012 confirmed after the fact the need of the platform to consolidate all its data about its users in one central place (Reitman 2012).

Google no longer promotes Google+ as its pervasive personal data collection and site of interaction. But the Google account is a thing that for the end user is separate from the Gmail account. The user registering to Google only uses it as a proxy to access another service or product. He may be creating a Google account to use his Android device. Perhaps he is attempting to use Google Docs for a collaborative project. The interface upon creating this new Google account makes it the nexus for several other sites of interaction.

Thus, the new user is not prompted to fill in his personal data directly into his Google account. Instead, Google will accumulate personal and behavioural data from several sites of interaction and build one comprehensive profiles from these. Unlike Facebook, it is not the network of connections to other people that matters the most for Google. What matters is the interaction with services such as Search from which Google draws a personal profile about each user.

Upon registration, the new Google account user is presented with a summary outlining the privacy and terms of usage with the account. If the user wants to, he can click on links for the Google's terms of services or the privacy policy. To fully register the account, the user must

scroll down the page and agree to the shortened policy. This shortened policy explains what data is processed by Google when using its services.

Although the registering user can explore the suggested documents in detail, the page flow design encourages him to scroll down the summary and agree to the terms or cancel the registration process. The terms of service and the privacy policy are opened in different tabs or windows. There are no parameters that the user can agree to or not. The page also appears like a pop up greying the interface behind. This choice of interface design reinforces the idea that interaction with the platform is limited until the user has committed to the agreement or not.

Some users may even be asked to confirm their identities, according to Google, for security purposes. In some jurisdictions like Canada, the registering user must enter a valid phone number from which Google will send a voice message or a text message with instructions to verify the account. For users whom Google forces to divulge a phone number, the registration will not proceed until that number has been confirmed. Google claims that it does this for security purposes and to reduce abuse of its platform (Google 2017).

During the registration process, if the user attempts to go back, most of the information entered during the registration process will be lost and he will have to try again. However, Google records data on the user's IP, browser, and make of the computer which will probably force the user to share a phone number again to complete the registration.

While Google claims that this strict verification process is to protect users, it requires a lot of personal information from new registrants before they have even had access to its platform (Google 2017). Unlike Facebook who favours obtaining data from users gradually, Google requests the date of birth, the gender, and the country of the registrant. It also requests a secondary email address or a phone number from registrants.

Google's verification process forces new users' flow to go in one direction with limited options as to what personal information they want to share. Requests for phone numbers are a development that Google, Facebook, and Twitter have introduced but that were not mandatory in the past. Older users of the platforms often get prompts to enter their phone numbers. Invariably, the justification for such requests is based on the need of the platform to secure access to users

and their personal information by providing an extra verification and security check based on a person's personal information.

A phone number is personal information whose purpose is the verification of identity. Access to the technological realm, however, is not dependent on platform's knowledge of phone numbers. Older users of these platforms can still interact and have access to most spaces involving no financial transactions without having to share their phone numbers. Platforms can still secure their users without needing the phone numbers of their users.

6.5.3 Twitter

Unlike Facebook and Google, Twitter was not created as a unique product by its parent company. Odeo Corp was a service company providing online podcasting services. Twitter, one of several projects from Odeo Corp, was created as an alternate dispatching system for taxi drivers. Twitter was built to be compatible with both the Internet and short message service infrastructures (St-Louis 2011). Twitter was not created to facilitate networks or for search. Before it was spun off as a separate company, Twitter was created by people who valued communication and broadcasting across several channels.

But Twitter's first users and clients were meant to be professionals such as drivers and podcasters. Compatibility with existing architectures was essential for Twitter's adoption. For example, Twitter's notorious 140 characters limit was designed to make its messages compatible with SMS infrastructures (St-Louis 2011). Registration and authentication to Twitter facilitates communications between users some of which are verified professionals.

An exchange between peers alludes to the communities of practices where users already know one another. Their identities and access to the technological realm has already been authenticated. Twitter's function is to facilitate interactions between peers. Messages stand as separate objects from their senders and thus form the use value of the platform. Twitter is the technology that allows broadcasters to reach their audiences.

Indicative of Twitter's origin as a pet project to allow struggling Odeo Corp to survive or produce a hit wonder, the platform continues to struggle with its role as the infrastructure

allowing broadcasters to reach their audiences. Instead of the broadcasters trying to commodify their audiences on the micro-blogging platform, it is Twitter which is compelled to commodify its user base for advertisers to survive.

Authentication and registration on Twitter allows the user to become both broadcaster and audience at once. The verification of the user's identity is to allow access to this interactive platform. However, Twitter's ongoing monetization predicament forces the company to gather information about its users in ways that seem more natural and logical for Facebook and Google.

When registering a new account, the new user is faced with a menu asking her to enter her full name first and then a phone number or an email address. Twitter asking new users to either register their phone numbers or their email address betrays its dual communication platform origin where SMS and the Internet are equal venues for users to broadcast their messages.

On Twitter, users' names are treated differently than the moniker used in messages. Users have a dual identity. The moniker is for messaging while the name is used for identifying the user. Instead of being a hidden piece of data, like on Facebook or based on an email address, like Google, the moniker (also known as handle) is how users access the platform. Every interaction with others in the feed is done through the moniker. **Table 34** demonstrates the different Twitter labels.

Table 34 - Twitter Labels

TWITTER LABELS	NAME	MONIKER (HANDLE)
EXAMPLE 1	Hervé St-Louis	@toondoctor
EXAMPLE 2	Johnny Bullet	@johnnybullet74

The sign-up page displays links to Twitter's terms of services, its privacy policy, and it policy on cookie uses. These are comprehensive documents that the registrant can easily access before entering any personal data in the sign-up page. This is a better display of policies than either Facebook which makes users accept a contract and adjust their settings after having registered or Google which greys out every other interface element and navigation from the user and forces her to scroll down a page to agree to terms before going forward.

However, there are still problems with Twitter's registration page. First there is an option for Twitter to offer the registrant tailored suggestions for their accounts. By default, this option is checked off. Again, if registrants want to understand what tailored suggestions are, they must navigate to a different page and read a policy document. Tailored results are based on tracking performed with third-party sites with Twitter tracking codes. In this document, Twitter mentions that users can uncheck this option and that any personal data about users begins to be deleted after ten days. Users can enable do not track features in their account as well.

The main problem with the Twitter login page is with the advanced options which are included in a hidden tab that appears to be another link that users may skip. These tabs hide two checked-in options where users agree to let others find them by their email addresses or phone numbers. The others could be other users, but it is unclear if they could also be third-parties such as advertisers. Because of the appearance of the tab, many users could enable this option without knowing.

Like Facebook, the current Twitter registration interface encourages users to let the platform import their contacts to help them find acquaintance that already use Twitter. The same networking needs that prompts Facebook to seek such personal information are at play. But for Twitter, this need is also a means of producing a ready supply of broadcasted messages to break new users' isolation. Again, the use value of Twitter is based on people's ability to consume messages. To support this use value, Twitter will even pre-fill a list of persons that a new user can follow, as well as making suggestions based on the registrant's topic preferences.

A secondary use value for more entrenched users is the ability to have a ready audience for their tweets. Gaining followers is a gamified process on Twitter where users with the largest audience gain more status and influence. On Facebook and Google, the number of friends and contacts a user has matters but it is not a status symbol the way it is on Twitter.

The process of creating a new moniker on Twitter is more difficult than on Facebook or Google. On Facebook, following the real name policy, multiple users can share the same name. The identifier that separates them in Facebook's platform is not their name. On Google, there are also difficulties when attempting to find new names. Much like domain names, all the good

names are already taken. However, Google allows users to use periods and other symbols for their email addresses.

Twitter's architecture only supports underscores and mostly letters from the Latin alphabet. At the same time, users must be strategic about the length of their moniker to have viable names that can easily be included in interactions with the network. Twitter uses another identifier attached to a user's account as monikers can be changed. However, they are not the visible part of the Twitter identity.

The process of generating a Twitter moniker is an important step in the socialization of the new Twitter registrant with the platform. Identities are valued on Twitter. Users are encouraged to fill shortened biographies of themselves to carve out a bit of property and to project their persona on the platform. Identity becomes a way for the Twitter user to advertise her broadcast channel to other users. In a few words, she must appeal to a wide audience and entice it to follow her, increasing the reach of her own messages.

6.5.4 Perceptual Evaluation Summary

The design model employed by Facebook in the development of its privacy policy is one where constraints on users' interaction with the platform are minimized to the extent that users do not have to see a privacy policy (data policy, as Facebook calls them) before they adjust their privacy and security settings. Meanwhile, Facebook attempts to gain as much personal information about its users even though they have only agreed to the privacy policy de facto. Responding to criticisms and recommendations (Denham 2009; Federal Trade Commission 2011; (Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic 2012; Fraley v. Facebook, Inc. 2013) from regulatory bodies and civil society, Facebook encourages users to adjust their privacy settings. But these settings are set against other users, not Facebook. Facebook's privacy policy is available, but users almost never interact with it directly. Instead, it favours a gamified version of its privacy policy that allows the platform to adhere to the broad demands of its critics.

Google's design model in the development of its privacy policy promotes the simplification of steps and information exchanged with users. Google forces new users to agree

to its privacy policy and other terms of services before they can start their registration process. However, summaries of the policy written in simple language are easy to find. These summaries are simplified versions of the main privacy policy that Google has already attempted to simplify and standardized across all its services and applications. While Facebook believes in omitting information about its privacy policy, Google attempts to make it as visible and present as possible.

Twitter's mental model is legalistic. Unlike Facebook and Google, during the registration process, Twitter offers opportunities for users to view the policy as is, without any modifications. Having presented its privacy policy plainly, Twitter focuses on helping new users navigate and become more comfortable with its platform. It presents its features and attempts to minimize the difficulty of securing a proper and unique Twitter moniker. The presentation of the privacy policy becomes a throwaway necessity offered by the platform operator but not an engaging part of its user experience, unlike Facebook or Google.

Twitter attempts to gather as much personal information from new users as possible before they use the site. In doing so Twitter forces users to interact with other platforms and systems making their interaction social and dependent on other sites of interaction. Facebook and Google also practice this. This practice adheres to what Dourish describes as social computing (2001). Social computing is about user interacting with several technologies socially as part of one activity. For example, Twitter users are encouraged to interact with their emails and contact apps. This forces users to synthesize information about themselves and other people through various interconnected technologies. When users adjust their privacy settings in a gamified environment, the activity they perform replicates gaming activity but in a different context.

6.5.5 Implications

Parametric privacy (settings allowing users to set and initiate controls for), confidentiality, and security settings should be offered by Facebook, Google, Twitter, and other platforms. They would control more than the data exchanged between users and some third parties. Such controls would allow users to decide overall how much data they choose to share

with the platform permanently. For example, users should be able to opt out of behavioural metrics that are used by platforms to track their interaction.

The end goal of registering users is probably not to spend time reading privacy and security terms of services when joining a platform. Authentication and registration become means to access a technological realm. By removing terms of services from the interaction flow of new registrants, Facebook adequately understands its users' needs. Yet, it could forego the collection of any behavioural data until users have agreed to the terms of services of their choosing. Google and Twitter could also do the same and only request access to data when it is needed. The need to know basis requirement for privacy is a longstanding principle in fair information policies (FIPS), and other frameworks derived from them, such as Privacy by Design (Cavoukian 2009, 2; Cavoukian and Dixon 2013, 12).[18]

6.6 Frame Analysis

With frame analyses of privacy policies, I seek to understand how Facebook, Google, and Twitter tell their stories about how they handle people's privacy and security. Frame analysis is an analytical method suggested by Goffman (1974) to understand the narrative behind practices and documents. I use frame analysis to understand what values and ideologies are represented by the privacy and security policies of Facebook, Google, and Twitter.

6.6.1 Facebook's Data Policy

Facebook prefaces its Data Policy (2016) document by stating that it gives the individual "the power to share as part of our mission to make the world more open and connected" This is a tricky statement. Facebook states its *raison d'être* in a similar way to Google's "*Don't be evil.*" Although a simple sentence, this mission statement orients all of Facebook's efforts. Instead of people giving Facebook their data, it is Facebook giving individuals an opportunity to give more information about themselves.

[18] Privacy by Design (PbD) is a policy-based prescriptive framework that encourages the integration of privacy measures within information systems interacting with users. PbD addresses more than the balance of competing interests of commercial stakeholders and their customers.

Except in its pursuit of its own mission, Facebook enrolls individual users without whom sharing would not be possible. What is not written implicitly by Facebook is that the user attempting to block this need for information to be shared, contravenes to an ideal and lofty objective for the benefit of humankind.

Facebook presents itself as a champion of access to information while omitting that this information stays on its own closed platform and is not easily accessible from the rest of the Internet. If an open and connected world was Facebook's mission, Google would have had access to its data assets years ago.

This self-serving mission frames everything that Facebook mentions in the rest of its policy. Facebook does not differentiate between information which genuinely can benefit humanity and that which is self-serving and not necessary to collect. For Facebook, all information, as presented in this policy seems to be of equal value and pertinence. Indeed, as much of this data is behavioural, its collection by Facebook is necessary. Much of this information is useless for the rest of humanity and only useful for user profiling. For example, the world has no need to know how many times my nephew has been watching and replaying videos of the *Annoying Orange* on Facebook.

Privacy can thus be understood as a rampart and a bulwark against Facebook's lofty objectives. Privacy becomes a necessary evil that the platform must contend with and include. Privacy is not treated as a positive thing nor is it mentioned negatively in the first paragraph where it appears after Facebook has stated its mission. If users want to find more about privacy, they can click on a link. And thus, privacy is dismissed and not put as the central item of Facebook's data policy. Yet, privacy still fairs better, as security is mentioned in the document only three times.

The privacy basics that the data policy sends people to is a series of tutorials and help pages where the user venturing this far can learn to gamify their privacy settings. There they can; choose who can see their pictures and posts; preview their profiles as another person would; determine if other people can see their friends' list; see who can view their likes and comments; who can see pictures that tag others; and, how to block and unfriend users. The tutorials reinforce

the game that users play with their Facebook accounts to encourage them to share. But of course, none of this stops Facebook from collecting personal data.

Instead, Facebook has performed the best *léger de mai*n in the social media world. It has sent weary users to a privacy game while obfuscating the fact that its data policy is its privacy policy. Except the label privacy has been excised from the title and morphed into something else. Facebook is choosing to frame its privacy policy as something else. It is a new category of policy that hides the negative connotations and restrictions associated with privacy and enlightens with the neutral term "data."

Having obfuscated its design from people to collect their personal information, Facebook then describes what kind of information it collects. It collects the following; information about what users do and information they enter on the platform; information others provide about users and interactions with them; information about who users are connected to and their networks; financial information used in transactions on the platform; information about devices used by users; information from third-party web sites and apps that participate in Facebook services and collect data for the platform; information from other third parties – presumably this is advertisers and data analysis third-parties; and information from other Facebook companies, or as defined in this study, secondary actors.

Here, Facebook is frank about what it collects although it seems to be trying to portray the situation as non-threatening. The most detailed description of its data collection practices is focused on the devices used by users to interact with the platform. The data collected includes device identifiers, locations obtained from GPS, Bluetooth, or Wi-Fi signals. It also collects IPS data, browser type, language, time zones, mobile phone numbers and IP addresses.

When describing how it gathers personal data, Facebook often uses terms such as providing, sharing, giving, and collecting. Facebook presents its need for information to build things. With this information, it gives something back to users and enables better experiences. It presents itself as a personal information assistant to people, anticipating their needs.

For example, Facebook claims that it is providing shortcuts when describing how it suggests photo tagging. It avoids the creepy aspect revealing that it inspects people's images and

comparing them to those held by other users. Rummaging through people's pictures with its own bots and comparing them to other people in their network or even outside of them is a benign practice for Facebook.

However, the amount of data inspection needed to perform tagging suggestions is extensive. It implies that Facebook is continually sending bots to inspect users' photos and comparing them to those of other people. Here, even if the user sets the privacy of his pictures to not be tagged or seen on another account through the gamified settings, major manipulation of personal data still occurs. It is not the other user who collects all this personal information. It is Facebook. There is a marginal operating cost that Facebook incurs every time a new user adds pictures to its platforms after registration. The continuing tagging of these pictures while being part of a marginal capacity cost is one way that Facebook monetizes its platform and absorbs marginal operating costs of users who timeshare on its platform.

User research is another area of Facebook's practices where the company highlights the benefits to users by arguing that what benefits itself, also helps people. In 2014, Facebook was involved in a controversy over an experiment it conducted on its users without prior participants agreeing or even being aware of the study conducted in their personal timelines (McNeal 2014). Facebook subsequently changed its data policy to include research as one of the ways it can use user data without full vetting by an institutional review board (IRB) (McNeal 2014).

Facebook differentiates using information from sharing it. Using personal information for Facebook is about internal uses for research, communicating with users, measuring ads and services. Information uses are direct manipulation and transformation of data. Sharing is about exchanging data with other parties be they advertisers, user metric firms, or other users. Information scholar Reijo Savolainen (2008) classifies people's interaction with information systems like library catalogues, archives, or the Internet as practices centered on the seeking, using, and sharing of information.

Still, these information practices, as Savolainen refers to them are performed by individuals and not organizations (2008). What is interesting here, is how Facebook uses softer words that are closely associated with people's experiences rather than technology to describe its

manipulation, analysis, collection, and exchange of personal information. For example, in its 2016 data policy Facebook writes;

> *"We are passionate about creating engaging and customized experiences for people. We use all of the information we have to help us provide and support our Services." (Facebook 2016)*

Elsewhere it writes;

> *"When we have location information, we use it to tailor our Services for you and others, like helping you to check-in and find local events or offers in your area or tell your friends that you are nearby." (Facebook 2016)*

Facebook does not portray itself as a corporation but as a friend who is rummaging through data the same way a friend on the network would.

Facebook's data policy sets the terms of a transaction where users agree to give more and more information to the platform so that it can be used to better target them. Facebook promises access and network connection to a technological realm whose denizens can probably be reached through other means. To justify the resulting commodification that occurs through personal information collection, Facebook wages a war with privacy going so far as to reframe the terms of engagement it offers to users. It highlights data which is a needed commodity instead of privacy which is an unavoidable process that platform operators must address.

The data policy differs in tone from Facebook's *Platform Policy* (2017) which is used to inform third-party developers producing apps for the platform. In this document meant for developers, which are not representative of the public targeted by the platform, the tone is more authoritarian. The document offers specific negative and positive prescriptions. Positive prescriptions take the form of; build this; follow that; keep this. Negative prescriptions take the form of; don't confuse; delete this; avoid that.

The regulations are written in a punitive manner that is meant to keep Facebook's third-party partners in line with the platform's objectives. This means that any practice that alienates or is counter to Facebook's mission of getting users to share is controlled. What is frowned upon

the most by Facebook are information sharing and use abuse that take the data obtained from users through the platform. Facebook is defensive of users' personal information and although it portrays any wrongdoing a slight against users, it is foremost a violation of its own privileged access to people's data.

An important document that explains how Facebook frames its data policy is the report it commissioned in early 2016 to a personal information consultancy. In the report, *A New Paradigm for Personal Data* (2016), the consultant, CrtlShift queried 175 participants whose work is related to personal data management. A total of 21 roundtables were held in various locations around the world.

CrtlShift held roundtables in the United Kingdom, France, Germany, The Netherlands, Poland, and Spain, the United States, Brazil, and Hong Kong. The roundtables in the United States represented all North America. The Roundtable in Brazil represented all South America. The roundtable in Hong Kong represented all of Asia-Pacific. CrtlShift did not schedule any roundtable for the continent of Africa, where Facebook users should also matter.[19] Some of the participants were academics or industry researchers but the majority of were from industry. There were a few government officials such as chief information officers. There were less than five participants who were privacy commissioners.

In the report on the consultations, personal data was treated as a commodity part of a new industry related to personal data management (CrtlShift 2016). Personal data is described as a value necessary for the economic development treasured by several stakeholders other than end users (CrtlShift 2016). The report describes personal data as important to many industries whose goals and needs are opposed with civil liberties defenders (CrtlShift 2016). Notwithstanding the debate on the nature of personal data, the report states that it is an immature market (CrtlShift 2016). Moreover, one of the goals of the report is to bypass regulatory controls over the use of personal data in favour of industry-designed standards (CrtlShift 2016).

[19] For example, Northern Africans have used social media to protest against their government during 2010's Arab Spring.

6.6.2 Google's Privacy Policies

Google's privacy policy (2016) focuses on the services it provides to users and attempts to explain in clear terms, without the typical allegories found in Facebook's data policy, what it seeks to do with user's personal information. For Google, this is a transaction where users use its services to search and share information but agree to let the Google platform understand and collect information about their practices (2016).

Google claims that this exchange of personal information with users will make their search results and the ads they are exposed to more relevant (2016). It also claims that this will facilitate connections with other users and make sharing quicker and easier (Google 2016). The document highlights search results, connecting with people, and sharing (Google 2016). The term 'ads' is not highlighted. Google here admits that its ads are not important for users or something that they need to be reminded of. Targeted ads benefit Google. The emphasis is on benefits to users. What benefits Google is not highlighted but should be understood as part of an exchange between parties. The currency is people's Google accounts and the personal data generated through them.

Google also signals early on that it attempts to keep its privacy policy "as simple as possible" (2016). It provides a list of key terms related to data collection practices that people can refer to at the end of the document (Google 2016). Through this, Google positions itself as a helper and friend who is not trying to deceive users and making them sign unwanted documents blindly. It presents itself as a mature and responsible corporate citizen that is playing fairly with users. But also, Google presents privacy topics as complicated issues that the average reader may not understand without its benevolent gesture.

Thus, Google frames its document as positively as possible and provides a counterpoint to other privacy policies that users may be exposed to. Transparency is presented as the platform's claim to fairness but also why it can request personal information from users to the extent that it does. There are no subterfuges.

Next, Google details and explains each of its collection practices, providing brief examples for each (2016). Some information comes from users and includes telephone numbers,

credit card numbers for transactions, names and email addresses. Google refers to these as personal information (2016). For most users buying services and making regular uses of features in Google services, while personal, this type of information is necessary for the regular operation of services.

But Google also mentions information it collects from users through the interaction with their services. This information, according to Google is not personal (2016). It includes; device information; log information; location information; unique application numbers tied to apps used by users; data in local storage; cookies and similar tracking information (Google 2016). Here, Google argues that only semantic information shared explicitly by users about their person is personal. Information and metadata gathered from interaction is not personal, according to Google.

This position is related to the personally identifiable information advocated by many platforms and advertisers about what is shared about users. Even though this information can easily be rebuilt to construe a person's profile (Barocas and Nissenbaum 2014), proponents of the personal identifiable personal information argue that they are protecting users and not breaching their privacy.

Oddly, Google does not perceive the broadcasting of some personal information across its network and services as a breach of user privacy. Google states that it may choose to display people's profile name and photos across its services (2016). Other information it may broadcast across its services are some user interaction with Google services like comments, and posts unless the user limits visibility options. Google also wants to share personal information from one service with others to increase sharing.

In developers' documentation on tertiary authentication, Google emphasized the ease of integration of its SSO process, as well as the potential gains third-party developers could expect after implementing authentication with Google in their apps and services. In three Google-authored case studies on tertiary authentication written for potential third-party developers, the platform operator touted the greater number of users completing full-registrations and returning

to the mobile apps using the SSO features. In the Moovit[20] case study, Google reported that 22% of users signed in using Google Sign-in or Facebook Connect (Google n.d., a). On Android, Google reported that 20% more users chose Google instead of Facebook for tertiary authentication (Google n.d., a).

In the Luxe[21] case study, Google reported that after implementing tertiary authentication with Google, the app's operators noticed a 20% increase in the registration rate and a 15% activation rates on Android and iOS devices (Google n.d., b). For Google, tertiary authentication becomes and important means to reach mobile users.

In its Doodle[22] case study, Google reports that Doodle's operators wanted to streamline authentication across all platforms and used Google's tertiary authentication processes. As well as a 50% increase from 35% in users signing in the app in Android, Google reports that Doodle's operators only spent one hour to implement the tertiary authentication process (Google n.d., c). Increase in usage is not the only benefit. Seamless integration and reduced development time for developers is the other benefit and a risk-free proposition.

Google features gamified privacy settings like Facebook but unlike the latter, it will let users remove information from their account from some of its services. It also allows users to opt out of some advertising services. Trackers can be blocked, although Google argues that exchange between parties will not work properly if some tracking is disabled. Here Google states that because both parties are not playing fairly that it will affect the quality of its services even though its technology, skills, and expertise are good enough to provide a seamless and great experience to users who decline parts of its tracking.

---

[20] Moovit is a mobile app on iOS, Android, and Windows Phone that allows users to combine crowdsourced live feedback about urban traffic with data from public transit operators to chart faster commuting routes.

[21] Luxe is a mobile valet and parking app.

[22] Doodle is a group event scheduling platform also available on mobile devices.

Just like with Facebook, Google incorporates its security policy and strategy within its privacy policy. While there are various settings that users can adjust to enhance their security, there is no standalone security policy like the privacy policy. Unlike the common perception of privacy as a component that I discussed in the Literature Review, Google more so than Facebook presents privacy as the wider concept and security as part of privacy (Mihajlov, Josimovski and Jerman-Blazič 2011; Bonneau, et al. 2012).

However, the form of information security that is described by Google does not adhere much to existing frameworks such as the Parkerian Hexad which models security as confidentiality, availability, integrity, possession, authenticity, and utility (Andress 2011). Information security for Google is about encrypting data and restricting access to its servers. These measures incorporate aspects of confidentiality which is the protection of data held in confidence, and availability which is about access to data that Google secures through authentication.

Google does not address issues related to integrity, possession, authenticity, and utility. Integrity is about the maintenance of data without unauthorized changes; possession pertains to the disposition of the physical media holding data; authenticity is about the genuineness and accuracy of data; and utility which is about the use value of data (Parker 1998). Google does have measures and incentives that address integrity, possession, authenticity, and utility but it is not presented to users.

For example, Google relies on a series of server technology that backs up cloud-based data continually. The integrity of the data users generated is maintained but it is not expressed by the company as an aspect of information security that directly matters to the user and the protection of their data. Similarly, Google offers measures to lock Android mobile devices that have been lost or compromised. This is an aspect of possession which again is not expressed as pertinent to users' security.

Google's framing of security in public documents like its privacy policy perpetuates what security expert Donn B. Parker (1998) refers to as the confidentiality, integrity, and availability bias. According to Parker, this bias reinforces a framing of information security as

being determined by privacy imperatives (Parker 1998). Parker argues that laws such as the *American Privacy Act of 1974* emphasized privacy and to an extent, confidentiality as the main threats against the public because the first cases of information security crimes were based on privacy breaches (1998).

Ulrich Beck's (1992) risk society theory can help us explain this fear of privacy loss. Earlier in the introduction to this dissertation I explained Beck's risk society theory as being pertinent to understanding information security and the context that surrounds this topic. Beck argues that risks are fears that humans perceive about potential negative outcomes and lack of controls over man-made changes to their living environment (1992). He writes that excess production and knowledge about the consequences of this excess in post-modern societies induces fears of potential threats (Beck 1992).

While production of wealth and goods is unprecedented, it creates other problems related to the abuse of common goods such as nature (Beck 1992). Knowledge about these risks is often portrayed as major threats to humanity (Beck 1992). Typical risks are related to environmental collapses, health epidemics and economic mayhem. I argue that concurrent with the advent of the information economy, risks induced by the proliferation of information and communication technologies also are part of the risks apprehended by post-modern humans. Fear of uncontrolled artificial intelligence, hacking, and cyberattacks are also seen as risks.

Parker argues that the folklore surrounding cybercrime has created distorted perceptions of risks in the public and with security experts (1998). Public officials, and governments who shape policy responses to information security risks should also be part of this list. These risks, while existing are not the only ones that can affect Google users. Yet, in its public documents, the company focuses on alleviating and minimizing those risks which seem more pertinent to the public while leaving out other matters which also affect users' privacy and security.

6.6.3 Twitter's Privacy Policy

Twitter's privacy policy is written in an active voice that describes how users interact with the platform, making collection of data from them a necessity. The company stresses early on in its privacy policy that that any tweet posted is public by default. The *raison d'être* of

Twitter is to be a public forum. This cannot happen unless the user understands that he should be as transparent as Twitter attempts to be in its document.

Transparency is also indicative of maturity. This is what Twitter expects from its users as it avoids sleight of the hand à la Facebook in its privacy policy. There is no cajoling users into releasing more personal information. People using Twitter are expected to know that the company will collect, use and share information about them. But these information practices are at the very heart of how the platform works.

Twitter's tone in the privacy policy is legal. It clearly identifies itself as a company and lists its address at the beginning of the document. It explains details about its international branch located in Dublin, Ireland. Some of the legal jargon relies on expressions such as "… you authorize us to transfer, store, and use your information in the United States, Ireland, and any other country where we operate (Twitter 2016)." Legal tones and constructions are not as apparent in Facebook or Google's privacy policies.

The structure of Twitter's privacy policy has not changed much since the first one it released on May 2007. Specific headings such as Information Collection and Use, Cookies, Information Sharing and Disclosure have not changed much. One major change in the September 2016 policy used in this study is the removal of a dedicated section for children. Unlike Facebook and Google, Twitter has not been a proponent of using gentle and comforting language in its privacy policy. The document's tone is clear, but still legal.

In several passages, the company asks users to be careful about what they choose to share on the platform, making people fully aware that they are responsible. Other times, it states that users can choose to divulge some personal information or not with the platform. Just like Facebook, some of this information allows the user to not broadcast this to then entire network yet is still recorded by Twitter anyway.

Here, the legal tone frames a discourse based on a transaction where all parties have access to the same information and thus must accept their responsibilities.

6.7 Transactional Token Analysis

In this section, I break the structure of the analysis that I have adhered to earlier in this chapter. I start my transactional token analysis with Twitter first. Twitter's policies and audience commodification practices are not as elaborate as Google's or Facebook's. Twitter relies on support from several third-party technologies to achieve its monetization of audience's attention. Because of this, applying the transactional token framework to Twitter first will also be easier to grasp. With a sound understanding of Twitter's practices, I can then explore how Facebook and Google perform the commodification of their audiences.

6.7.1 Twitter

Twitter designed its authentication process so that users may be tracked even when they have been logged out. A check box with the inscription 'Remember me' suggests that tracking will continue even after the session, thereby increasing the reach of the commodification process happening to the user. The current home page that people log into features Twitter's Moments. Moments are snippets from popular tweets and events happening and being tweeted about. Moments echo both internal Twitter interactions between users or responses to world events. Moments are geographically-matched to the user's location and organized into topics.

While no advertising is present in Moments, Twitter is attempting to grab users' attention even before they authenticate. Remarkably Moments do not convey a call to action encouraging users to perform authentication to interact with contents. However, if the 'Remember me' option was checked in previous sessions, Twitter will be aware and able to identify the user and target moments specifically to her. But once authenticated, any interaction with moments is tracked, whether previous sessions were tracked or not.

Identity verification can proceed with either a user name, a phone number, or an email address. Unless the user was viewing moments, once access to the technological realm has been granted through identity verification, the user is taken to her Twitter customized timeline. At the time of the analysis, Twitter relies on its own tracking and that of external parties, including Google. Twitter uses its own Twitter Analytics tracking, Google Analytics, and TellApart.

Twitter Analytics tracks user tweets, their impression, profile visits, and mentions. But it also tracks information related to audiences interacting with an account. It provides demographic information about audiences' interests, lifestyle and site of interaction such as desktop, laptops, tablets or mobile phones. Some of the data Twitter Analytics can reveal to a user is the gender balance of followers, if they like movies, sports, or comics, and language used.

Google Analytics provides similar information but unless the user is also authenticated in his Google account, specific data may not be available. It is unclear if Google Analytics has been modified for Twitter's architecture. TellApart uses predictive data collected from several sources to create personas of users interacting with platforms. It helps companies convert potential Internet uses into targeted consumers.

Through its syndication platform, Twitter Syndication, the microblogging site places syndicated promoted tweets from advertisers within users' feeds. The syndicated tweets have been generated from data generated and aggregated from several other sources including Twitter and other sites. For example, they are used to design profiles which are then targeted and exchanged with Twitter and other parties. They are then reused in either opt-in and opt-out tracking. It is when the user performs an authentication through Twitter, that this data can then be used within a syndicated tweet presented to the user to monetize their attention. The audience member will either choose to view the promoted tweet; interact with it by resisting it; erroneously interacting with it; or buy-in the message.

These promoted tweets still compete for people attention against a plethora of notifications and tweets coming from the user's feed. Notifications and tweets are part of Twitter's use value and how users interact with the platform. Recognizing this, Twitter has placed ads where these interactions thrive. There are promoted tweets embedded in retweets and the notifications tabs on both the desktop and mobile apps.

Here, I have described a commodification process which did not start at monetization of attention. It started at the data generation and aggregation stage instead but still looped back in the entire process and used authentication to allow the monetization of attention to occur anew.

This process is recursive. Twitter uses its own data gathered from user interactions but also from third-parties such as predictive marketing firms like TellApart.

As argued earlier in the perceptual evaluation of Twitter, the platform enables users to become both broadcasters and audience members at once. Twitter plays this difficult role of trying to encourage some of its audience members into becoming advertisers. The Twitter Analytics tools plays to audience members seeking to augment their reputation as if it were a property (Post 1986). It is also a launching pad for potential advertisers who will thus pour money into the platform.

The advertiser here is just a commodified audience member who fits in a new class but at his root is still a user. Part of this is possible through the corporate presence that a platform like Twitter is uniquely positioned to accommodate. Better than Facebook where groups, firms, and institutions can create profiles and sites of interaction within the platform, on Twitter, these same actors are nearly non-differentiated from individual users.

Twitter as a platform can thus present itself as an intervenor to connect audiences and broadcasters. The user profile is simpler to generate than a full Facebook site of interaction. The user profile on Twitter is not a mini-website like the Facebook profile. It is the account of a person, the human or a moral person. Moreover, even fictitious and parody accounts can easily thrive on Twitter. Parody accounts are much more difficult to maintain on Facebook where the existence of an account requires more effort than user-to-user interaction.

Although Twitter as a platform is a site of interaction by attempting to track its users even after they have logged out, it seems to perpetuate the ephemeral technology where audiences dwell. The tracking which remains with the platform follows a user which was once authenticated and interacting directly with the platform. But through cookies and other semi-permanent trackers, Twitter can follow this person. However, the person has ceased using the platform directly. The person no longer has access to the full technological realm of Twitter's platform. Yet the user's identity is partly verified and tracked for continued commodification.

The trackers that follow the user after he has logged out continue to prepare and customize his ephemeral technological realm for the next session. Identity verification happens

through the collection of more data based with the individual's interaction with other third parties. But the user obtains no further access to technological realm outside of Twitter. What is occurring instead is that Twitter, and other third-parties benefit from the exploitation of the user's personal data and interaction. Like cattle, the user is branded only to be consumed later by a producer.

Even when away from Twitter, the user through his account is using private property. Specifically, it is a timeshared property where both the broadcaster and audience members use. As the once authenticated user continues to be tracked outside of Twitter, his traces offer him no property rights protections. The data his interaction with third-parties generate are not protected for privacy or security unless he enables 'do not track' features which may or may not totally shield him from tracking. Some data like the device that he uses will still be tracked.

His identity is recreated through traces generated by his lack of privacy and security. This data can easily be exchanged with third-parties such as TellApart by any site of interaction he visits. This form of identity data is created negatively, and not explicit information shared by the user. As such, it is not the kind of data that used in APIs designed to enable tertiary authentications.

6.7.2 Facebook

Contrasting Twitter whose content straddles the line between being opened and closed, Facebook shuts off people who have not logged into its platform. Its privacy and security settings also shut non-authenticated users from viewing the timelines of users who have chosen to protect themselves. To experience Facebook, one must be logged in.

But once she has logged in Facebook, the user is served a controlled environment that Facebook customized to gain the most from her attention. Twitter still allows users to view their feeds chronologically even when it attempts to disturb and encourage them to view targeted posts and follow specific users constantly. Facebook users don't have that choice. Just like when they visit Disneyland, a corporation attempts to control their entire experience and make them stay as long as possible. Disney attempts to make visitors consume and spend their money. But Facebook wants users to spend their attention on its platform as long as possible.

Unlike Twitter, Facebook does not ask its users if they want to continue being tracked by the platform after they have ended a session. Facebook continues to track its users, as demonstrated by photographic log in option that allows users back by using their profile picture to access the site. Potentially, this means that users' interaction in other venues that participate in Facebook tracking are also recorded by the platform.

While Twitter attempts to classify the likes and dispositions of its users, Facebook aggressively seeks to organize its users based on every metric it can find, be it religion, political ideology, hobbies, age, marital status, profession, education, location, and history. Beyond a simple verification of personal information such as phone number, name, and email, Facebook attempts to fill as many information gaps about its users as possible. The technological realm that the user sees is created just for her and is based on the information that Facebook collects.

Advertising is almost inescapable on Facebook. Unlike Twitter, Facebook relies on its own tracking tools almost exclusively. They are not easily recognizable by browser-based anti-monitoring technologies that seek to limit the invasiveness of Facebook. The platform inspects every interaction and every piece of data generated by its users. One tracker used by Facebook is Atlas. Atlas tracks users across devices and domains. It appears to be implemented on Facebook's homepage before the user has even logged in.

Once logged in users will see ads embedded in their timelines and on the sides. Facebook keeps its users perplexed by deliberately mixing targeted suggestions for new groups, clubs, and organizations with advertising. It creates an advertorial mix where users have more difficulty discerning advertising from benign suggestions. This is more aggressive than Twitter where promoted tweets are clearly indicated as being sponsored. This practice can be explained as form of design and profiling of users.

Design and profiling increases Facebook's ads hit views but also maximize the response to calls to action desired by Facebook. Blocking an ad may mean blocking a genuine topic of interest. If the user interacts with a non-advertisement placed in the same advertising space, the data from the interaction and the interest will still allow Facebook to better profile the user while minimizing user resistance to ads.

Facebook works with a few third-parties with whom it exchanges some advertising-related user behavioural data (Facebook Business 2016). Tertiary app and service developers who want access to user data stemming from Facebook's targeting can obtain some through various schemes such as the Facebook Login API. Some of the information available includes user relationships, religion, politics, tagged places or even likes (Facebook for Developers n.d.).

Advertisers and tertiary app and service developers who want to connect with Facebook's user data and authentication must create individual accounts first, before they can create groups, corporate, brands, or institutional pages on the platform. Whereas Twitter allows non-individuals to create accounts and interact with other users directly, Facebook forces a second level of registration to its platform. Individuals must create sites of interaction first before being accessible to users. These non-individual sites of interaction must be manned by users with Facebook accounts. Just like Twitter, the advertiser and the common user can exchange role, produce and consume.

As soon as the site of interaction has been created for a non-individual entity, Facebook will encourage its operators to advertise their destination to obtain more visibility and to reach other conversion goals, such as sales, and customer support. This non-individual site of interaction becomes a new class of Facebook users. It is one that Facebook advertises directly to. The direct advertisements reach the individual account of the person.

Facebook's strategy seeks to retain users' personal information even when they present themselves to the public as corporations and institutions. Twitter loses that information to the extent that a new registrant can use a corporate email address or phone number. Facebook does not lose anything. The value of the site of interaction's operator may be minimal though.

Facebook uses timesharing to give the operator of a non-individual site of interaction a space to reach other users. The user generates data both as an individual and as a representative of an organization that remains on Facebook and adds to the use-value of platform. Facebook treats it platform as its exclusive property requesting that users be authenticated before obtaining access. But the value of authentication enhances the accumulated value of Facebook through its users' labour without directly preserving security and privacy.

Facebook is aggressively attempting to change its use value from one where users and their peers entertain one another and consume each other's contents to one where corporate and institutional actors create a presence within the platform's closed doors and forcing interaction outside of the open Internet. Zittrain describes this closed system as one where security usually prevails over innovation and generativity (2008). Third-parties play by the rules set by the closed platform operator.

However, security is not necessarily assured when using Facebook. As I described in the perceptual analysis of Facebook, security is part of a gamified experience where users adjust their settings. There are no common security settings and features that prevent users account to not be compromised. There are no security vetting processes by Facebook like Apple's iOS App Store where tertiary apps and services are verified before being offered to the public.

6.7.3 Google

Google, like Twitter and Facebook is attempting to create a platform where it can retain its users as long as possible so that it can monetize their attention. Google appears to rely less on authentication to commodify audiences' attention. Authentication is omnipresent at Google, just not at the level of abstraction one expects.

Google's main draw for users is its search engine. This search engine has been available since 1998 without requiring users to authenticate themselves to use this technological realm. A simple Google search will yield results but also AdWords advertisements that match the user's location, his search query, and allow the platform to collect other behavioural and interaction metrics.

It is only when Google began adding other products and services that authentication became an issue. Authentication became a way to verify users' identities and enhance their profiling and the targeting of ads aimed at them. Still many of these products such as Google Docs, Google Translate, and Google Forms display no advertisements in their interface. Users do not need to login to use them or modify files, if access options enable file modification.

Other services such as YouTube can be used by users without authentication. Authentication was originally aimed at users who authored videos for sharing on the platform. When Google added mobile apps, it attempted to make authentication a default for usage, thereby avoiding the open access platform that it popularized on the desktop.

Google Gmail is one of two services that by its nature forces users to verify their identities to gain access. Google does monetize Gmail by relying on users' input and labour to profile them and serve them advertisements based on the contents of their emails. Google actively scans, and monitors users' emails and targets them with ads based on what they read and write in their mailboxes.

The other service is Google Android. Google decided to create a closed platform with Android, forcing users to authenticate themselves on their mobile devices and be logged in continually. Google could have chosen to not make authentication the default and to tie its mobile operating system services and features to its servers and advertisements. Instead, Google actively encourages the commodification of its users using Android devices.

Through Android, Google can test new products, perform measurements of its users, understand their location and usage of their devices. Everything a user types and searches for is recorded by Android. People's contacts, usage of various apps such as SMS is monitored by Android. People's locations are always known. Which network they use, whether it is a mobile or a WI-FI network is known to Google. Users have almost no privacy from Google when using their Android mobile devices. I will explore the consequences to privacy in the context of the transactional token below.

Authentication with Google works on several levels that can be readily explained though the transactional token framework. Having already explored how the monetization of attention works with Twitter and Facebook above, I will demonstrate the various levels of abstraction at play with Google authentication. But before doing so, here is a brief description of the monetization of attention with Google.

How Google monetizes the attention of its users through its Search and other services is like how Twitter and Facebook commodity their users' attention. It involves the presentation of

ads in the interface used by users, leading to either hit views, or calls to actions. These are advertising interactions which users react to by resisting, performing errors, or buying-in. The data generated from the advertising interaction can be discarded, ignored, or used to design and profile user personas. These personas are targeted by Google and the data exchanged with advertisers, audience monitoring firms, or third-party developers using the data as part of their tertiary authentication processes. However, every tertiary authentication relies on the primary authentication into Google.

Primary authentication into a Google service or product is one way to access Google's platform. However, as I argued in the theoretical framework chapter describing the transactional token, being logged in assumes that one was logged in in a prior different level of abstraction.

Even if the user is not logged into Google, he is still authenticated in the platform. Authentication gives him access to an ephemeral technology where he can search for terms, watch videos, perform translations, browse through images, etc. Before I make my claim that one can perceive access to Google as both access to private property and public commons, I will explore how using a platform like Android seems to negate the concept of an ephemeral technology where access is limited to temporary sessions.

Android, like other current operating systems such as iOS, and Windows 10 attempts to create an environment to convince their users to remain within their own playground. The operating system becomes the totality of the experience of the user on the platform. It is always in the background, monitoring the user's wants and needs. Personal assistants become part of the strategy to reinforce the totality of the user's interaction with the device.

While they can be deactivated like laptops and desktop computers, such as tablets and smartphones, chances are that mobile devices are almost always running. Yet the concept of an ephemeral technology where users interact with a technology they have authenticated in through sessions with temporary durations is still a valid description of authentication with an Android device. Authentication can only happen if the user's identity is verified. Without verification, the user loses access.

As I argued in the theoretical framework chapter, there is no set duration for a session. But eventually all interactions with an information system into which a person has authenticated himself will be finite. A user may use the same Android phone for three years, until it is replaced by another device. In that time, the phone will have been shut, crashed, or be out of power at least a few times. These are the ephemeral moments that limit the sessions with a technology.

However, the ephemerality of technology easily hides the fact that users were already authenticated at a different level of abstraction allowing them access to the Android device. For example, authentication could be with the contract entered with a cellular service provider like Bell Canada or Sprint. Many times, devices must be registered with a mobility service provider and are associated with one user. This is authentication on another level of abstraction that occurred prior the use of the Android smartphone. Ephemerality of technology means that there is always another level of authentication where the verification of identity leads to access to a technological realm.

The level of abstraction where the authentication occurs beyond the Android device can be a private or a public property. As a platform operator, Google is a private property owner exploiting its search engine. Google's search engine is operated by a corporate entity, but it is also possible to argue that the ubiquity of Google's search engine and the rate of usage with the public almost makes it a public good, like how telephone operators are granted rights to exploit public airwaves. The closest regulations that affect how Android is deployed by Google are privacy acts such as Canada's PIPEDA (Minister of Justice 2015).

Since access to Google's search engine does not require authentication, the monetization of users' attention happens differently, while requiring the identity verification of the person that will grant her access to the platform. The user performing a search on Google is accessing the resources of a private property that Google has the exclusive right to exploit. The use value of this property is to perform searches and display results to users. Because Google enabled search-related advertising in 2003 in the form of AdWords, another use value of the search engine for Google is to profile users and target them with custom ads.

Regardless of the penetration of Google search with desktop and mobile users around the world which in the United States, particularly hovers around 64% (comScore 2016), the platform is not a public common. Google relies on a shared resource, which is the telecommunication network that shapes the Internet (Newman 2010). But because of the ubiquity of the Google Search, I want to perform a brief analysis of the platform as if it were a public good because of what it can tell us about commodification and authentication.

Public Commons are public goods owned by all. They are an abstraction level beyond that of the ephemeral technology. For example, if Google Search is considered a public good, log in from Google Search into a Gmail account would be interacting first with a level of abstraction beyond the email service and then starting a session with an ephemeral technology. For the user to have access to Google Search, she must first be authenticated. Access is provided through her Internet connection, her computer, even the very facilities and space that she uses before she reaches for a computer.

David Clarke's (2012) control point analysis becomes an important method underlying my transactional token framework. Each step before accessing Gmail requires a level of abstraction that requires the user to authenticate herself before going forward. The Internet, like Google Search is a difficult case to classify as it acts like a public good. In some jurisdictions, like Canada, access to the network is embedded in law (CRTC 2016). As a public good, its infrastructure is governed independently of states and is not meant to benefit corporate interests. Yet the network is owned haphazardly by several actors.

To access the Internet, and then Google Search, the user requires a computer that adheres to specific networking standards giving her computer entry the rest of the network. This adherence to standards is a form of authentication. Without the right standard, verified by network peers, the computer cannot access Google Search nor the Internet.

However, the adherence to a technical standard is not a recognition through a community of practices. I have argued in the theoretical framework chapter that authentication can happen through peers only with human-to-human interaction when it concerns public commons. Communities of practices, in the context of authentication are embodied practices between

humans. Peer-based recognition based on technical and instrumental standards are analogous but not based on communities of practices. They lack the human experience and context that qualifies such interactions. Recognitions based on standards are best understood as peer-based authentication grounded on shared technical standards.

With peer-based authentication using shared technical standards, the user's personal information can be embedded or not within the computer. Google Search at the very least can verify much about this "anonymous user" before she even logs into her Gmail account. Now, Google Search is not a public good. The platform is private property yet, much like a lot of the Internet infrastructure, its acts in many ways like a public good upon which people depend. Looking at Google Search as enfranchised space helps.

As I described in the theoretical framework, enfranchisement is a practice to curb state power over individuals and by extension, corporate entities like Google. Looking at Internet governance, there is a strong parallel of this. In 2016, the U.S. Department of Commerce withdrew its direct control over the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is the top-level Internet-related governance body in the world. But ICANN and other Internet governance organization are not enfranchised. Enfranchisement is a limit on state power, not a complete relinquishment of state oversight.

Enfranchisement involves a legitimate claim by civil society elements to curb limit state oversight. It is also an act of authentication where the state provides a license to the enfranchised party to exploit certain rights or a property. Google has such a right regarding the exploitation of its search engine. Were Google Search deemed monopolistic as it were in Europe in 2015 (C. Williams 2015), the state could fine, break up, or severely limit Google's exclusive right to exploit its own platform.

6.8 Conclusion

The current architecture of tertiary authentication is built mainly with OAuth standards. It is how primary platform operators like Facebook Google, and Twitter allow their users to register to their platforms. One key aspect of these new registrations which forces platform operators to incur marginal operating costs is to gamify the interaction with the platform

whereby any action performed by the user can be recorded. The metadata from this interaction helps operators monetize their platforms. Thus, the act of consulting a privacy policy or a term of use offers an opportunity to platform operators to collect metadata on how users interact with information systems. This has encouraged them to maximize the presentation of privacy policies and terms of use so that they are no longer just legal contracts outside of the experience of users with a platform, but components of the interaction and experience users have as they visit Facebook, Google, and Twitter. The framing of the role of privacy, confidentiality, and security has thus changed to serve the interests of platform operators, better as demonstrated with the transactional token framework.

In the next chapter, I discuss the implications of the commodification of user's personal information through tertiary authentication by merging insights from the quasi-experiment and the policy analysis performed in this chapter and in Chapter 5. Chapter 7 answers the question of whether the three research questions of this dissertation have proven correct.

Chapter 7
Discussion

In this chapter, I merge the insight gained from the evaluations of the two previous findings chapters dealing with the policy analysis and the quasi-experiment performed to answer this study's three research questions. They are;

a) What is the extent of the interplay between security and usability for platform operators that are commodifying from users' personal data through tertiary authentication?

b) How are people managing and controlling their security and confidentiality as they perform tertiary authentications and what are the implications of those actions for users' perception of identity and privacy?

c) Which conditions and variables create a perception of false security in users performing tertiary authentications, and what factors of tertiary authentication affect users' sense of security?

The purpose of policy analysis was to the understand trade-off between security and usability of platform operators that profit from tertiary authentication. The quasi-experiment's purpose was to answer how people manage and control their security and confidentiality as they perform tertiary authentication and to understand the implications of those actions over users' perceptions of identity and privacy. The quasi-experiment was also needed to unearth which conditions and variables create perceptions of false security in users performing tertiary authentications and what factors affect their sense of security.

7.1 Research Question One: Background and Motivation

I will now answer the **RQ1** of this study starting with a brief overview of the problem space. In this study, I have used the transactional token framework to frame my evaluation of the interplay between security and usability in the commodification of users' personal data during tertiary authentication. I claim that the tensions between usability and security which are the hallmarks of usable security cannot be solely understood as a tension between two sets of values pitting the security of data with user convenience (or usability).

Both values are practices that exist in a context where platform operators must profit from their endeavours to survive as corporate entities. Facebook, Google, and Twitter are not public goods. They are private enterprises whose private property they have the exclusive right to exploit. During their business operations, Facebook, Google, and Twitter have chosen to support the costs of operating their businesses through ad-supported schemes instead of subscriptions or pay as you go services. The valorization of these companies is built on their ability to convert information into products sought by both users, advertisers, and other marketers.

The information produced by users is what attracts other users whether it is found on a social network, a search engine result, or a micro-blog. Users go to Facebook to consume the information produced by their network peers. They also consume the information promoted by third-parties or referenced by their network. Users seek the information produced by users in websites which are referenced by Google and other search engines. Google presents a proxy of this information on its platform, allowing people to decide which offer they will pursue. Users consume the information produced by other users on microblogging sites like Twitter.

Incidentally, the network effect of so many people in one place creates the potential for an audience whose attention is apt to be captured by advertisers through their own contents. Both marketers and advertisers are interested in the metadata produced by users as it enables them to better design and profile potential customers, before targeting them. But without people aggregating to a platform, there are little opportunities for advertisers and marketers. Hence platform operators must foster sites of interaction where semantic information and metadata can easily be generated by users and commodified so that it can be resold to advertisers and marketers.

Two forms of labour are involved in the production of the platforms developed by Facebook, Google, and Twitter. Some of this labour is produced internally by their staff and other workers on their behalf. But the classic labour of workers exchanging their work, and time against wages is supplemented by the labour of audiences using the platforms. The information generated by audiences is labour that can be commodified. Users interacting with Facebook, Google, and Twitter generate data in the form of semantic information that they inscribe in the

platforms that they use. But they also generate data in the form of metadata produced through their interaction with information systems. This metadata is not produced consciously by people. But it is still a bi-product of their interaction with platforms.

Facebook, Google, and Twitter must be understood as sites of interaction that are timeshared properties where people are granted personal space to exchange with others. However, this space does not belong totally to users. Various platform operators have varying policies to claim some of the data, personal, or public, generated by people (Rigi and Prey 2015).

The impetus to profit from users' data is caused by the marginal operating cost of every new user and the marginal capacity cost incurred when hosting people's data. Marginal costs force us to consider the scarcity of online space. Online space is not limitless. For example, several Silicon Valley start-ups rely on cloud-space provided by vendors such as Amazon, or HP. Platforms and their maintenance are gigantic operations that require a constant shuffling of data across resources to maintain the physical integrity of the hardware they are recorded on and the logical authenticity of the data itself.

While the integrity of hardware and authenticity of data appear to be classic components of security paradigms alone, they also raise questions about usability. Security is not as much as a backend concern when it must allow users to use data held in confidence by platforms on people's behalf. Security must be usable so that at the frontend of platforms, users may interact with the information that they produce, and the information produced by others. The quality of this interaction is a usability problem.

Security is a vague concept in information security. As I have discussed in the Literature Review, security can be either personal or perceived about concerning organizations and states. In the context of platforms that users interact with, security is a concern at the individual level and the organizational level. It is not a matter of politics, war, or terrorism. Security in this context, is grounded in the realm of civil society.

Security here is about the interface between the user and the data that she produces, that she seeks, that she uses, and shares. The interaction of people with technology invariably raises issues about usability. If the security of the data held in confidence is questionable, it is not only

a security concern for users but a usability concern. Even if the physical integrity of the hardware and logical authenticity of the data were sound, if people cannot access this data or perceive that they cannot, this is a usability challenge borne out of security perceptions. I am arguing that security and usability when it comes to user interaction with platforms is a recursive and dialectical relationship where both phenomena are parts of the answer that shapes people's perceptions.

Platforms operators have incentives to exploit people's data which they hold in confidence. This forces Facebook, Google, and Twitter to provide security and usability measures to the user data they hold. How this is expressed is more practical than the theoretical perspectives that I argue here. Usability and security are still perceived by some platform operators and other industry actors as two dialectically opposed streams that must be integrated in a way that allows both values to fulfil their expressions and roles. Convincing enterprise actors that security should be built in at the core of their product was a challenge of a generation ago. Today, the same enterprise actors are finally accepting that usability is also a value that matters as much. The next challenge is the integration of security and usability as one value. I argue below that this integration is happening but not in a classic usable security scheme.

The site of interaction where usability and security are easier to observe and where users' perceptions matter the most is the site of authentication. Authentication is the prerequisite practice that accompanies people's interaction with technology. In this study, I have argued that when people interact with technology, they perform authentication. This authentication does not have to be happening now. It has already happened as the person has most likely verified his identity at a different level of abstraction before being granted access to a technological realm that would allow him to interact with a current technology. In this study, I have labelled this current technology, the ephemeral technology.

The ephemeral technology is the one the user interacts with when using Facebook, Google, or Twitter. But it is not any kind of ephemeral technology when we are discussing Facebook, Google, and Twitter. This technology is private property. It is a timeshared property. Users generate data which at any point can be commodified to attract advertisers and marketers.

7.2 Research Question One: Answer

The traditional way of understanding the tension between security and usability, or an interplay between the two, would be to argue that the more secure a platform is, the less usable it is for users. This interplay takes the form of a trade-off. Security, as traditionally designed creates barriers that users would like to circumvent or that will keep them away from the platform. Consequently, the more usable a platform is, the less secure it would be as security measures would have to be sacrificed for usability's sake. While I do not dispute this phenomenon, there is a deeper and more paradoxical tension unearthed by tertiary authentication.

Tertiary authentication, as we have seen in the Technical Background Analysis of the Policy Analysis, was engineered to answer both security and usability problems. The original single-sign-on utilities (SSO) were created to provide enterprise users with a single site of interaction to perform safe authentication. However, both security and usability, were ultimately provided at the behest of enterprise operators who needed more control over the labour of their employees. Just like with the efforts of WWII engineers to redesign cockpits of aircrafts for pilots (Grudin 2012), usability, or at the time, human factors were a way to streamline labour and maximize the value of that labour (socially necessary labour time).

And so, it appears that the trade-off between security and usability can be best understood by considering that both tensions are heavily affected by capital accumulation. Capital accumulation as described in the Theoretical Framework is the process of accumulation of wealth through people's labour. SSO and its current form in tertiary authentication are the results of the trade-off between security and usability.

7.2.1 Technical Background Discussion

The main observation that I draw from the technical background analysis of tertiary authentication processes is that changes in interaction modalities favoured OAuth as the technical solution to enable tertiary authentication. Mobile interaction where older solutions like OpenID, created to facilitate usability with the public, were limited to browsers. OAuth was not built for tertiary authentication but for authorization. But it was an acceptable compromise for

platforms seeking to expand their reach in the mobile realm and to foster an ecosystem of tertiary apps using their infrastructure as their backbone.

But Twitter differs from Facebook and Google. Twitter continues to use OAuth 1.0a which has limited usability for developers. OAuth 2.0 was developed to enable authentication as well as the sharing of authorized resources.

An important trend that can be observed is that Twitter no longer pursues a policy of fostering clone clients (O'Dell 2011). Facebook and Google have not focused on promoting clone clients as they want users to remain in their platform and to consume and produce information there. Facebook promotes tertiary services that allow users to stay longer. Google and Facebook promote the SSO through their platform to be able to amass more behaviour metadata on their users and to facilitate their monitoring when they venture outside of the platform.

The emergence of OAuth was caused by changing interaction modalities. Ubiquitous computing means that the modalities and sites of interaction are no longer just browser-based. Mobile usage is now a major source of user interaction with platforms. For Google, Android is at the center stage of its industry dominance.

When observing the emergence of OAuth as the premier process for tertiary authentication, the trade-offs between security and usability are weighted on usability. There are security risks and flaws in both versions of OAuth, but these are mostly ignored in favour of the utility that the standard provides to platform operators.

An interesting insight revealed by the technical background analysis is the place of OAuth as a critical part of tertiary authentication. OAuth is the backbone of an entire socio-technical ecology and business model based on the commodification of people's attention and labour. It is a security risk in the making that could unravel quickly if brute force was used to compromise it. Brute force attacks are dedicated outbreaks where numerous passwords are tested against an authentication system to allow a perpetrator to break in (Ristic 2010).

The revelation of the critical role occupied by OAuth is significant because tertiary authentication will only grow and not go away. It maintains the hegemony of platforms. It is necessary for Twitter to be attractive as a path for tertiary authentication or it will lose its status as one of three main platforms. Microsoft and Apple also have tertiary authentication, but they are tied in part to an operating systems and alternative technological solutions. In the past, before ubiquitous computing made it an imperative, Microsoft lost its head start with Passport, its SSO solution. Apple uses iTunes but attempts to maintain it as an internal solution, or in other words, a secondary authentication process. It favours the closed platform approach.

7.2.2 Perceptual Evaluation Discussion

A major observation is that for Facebook, security and privacy are elements to foster user experience that will promote the sharing of more information. When a user blocks another on Facebook, the act becomes a metadata point of relevance for the platform operator. It provides more insight about the relationship between the two users, just like a like or a photo tag would. Hence Facebook has produced a wholly integrated security focused mostly on privacy, which is the main concern of its users. Security and privacy are aspects of user experience and by an extent usability.

Google’s challenge is both security and privacy. Google accounts can be hacked. At the same time, concerns about Google’s handling of people’s privacy are recurrent. Google's interaction flow for registering users is more stringent than Facebook's. Whereas registering Facebook users can play with the platform, for new Google users, most features and options are closed until the interaction path has been completed.

Security and privacy policies are not hidden from users. Settings are not gamified against other users and third-parties. They are set to protect users from Google and hypothetical enemies such as hackers, and criminals. But Google can still collect data from users through its various apps and services. Users can delete some of the personal data collected about them, but it is unclear if it affects the profiling performed by Google.

Twitter attempts to make its platform palatable for new and experienced users to encourage continuous use. In doing so, it attempts to facilitate user interaction with the platform.

But Twitter also attempts to provide basic security to users by having them confirm their identity by adding their personal data. The risks with Twitter are mostly based on compromised Twitter accounts spamming other users. Interestingly, this is not exactly the problem usually associated with Facebook. Facebook's challenge is privacy.

Privacy at Facebook serves usability objectives. It is not directly available as a document. Instead it is available as a series of tutorials and other literature that demonstrate Facebook's commitment to privacy. Instead of browsing through a legal document, users can explore.

Like Facebook, apps and services appear to collect information about users to profile them and then target them with ads. Google plays a different longitudinal game with people's personal data than Facebook. Whereas with Facebook, every site of interaction appears to solidify existing user profiles, Google seems to be interested in what people are thinking and doing in the present so that it can best serve them relevant ads.

Facebook seems to build long-standing user profiles that can predict future interests or major life stages. Google just wants to know to what restaurant the user will be interested in the next hour. If Joanna searches for restaurants, she will be served with restaurant ads. Where a systematic preference for Mexican might be an insightful data point for Facebook, with Google, restaurant preferences from two years ago seem less relevant.

Twitter is trying to profile its users so that it can match them with relevant posts and other users as well as target them with appropriate advertising. While Facebook also prompts its users to add more people they may know to their network or join specific groups, Twitter encourages additions based on people's interests and who they have interacted with recently. Twitter is interested in the networks people build and does use that information and contents of tweets to improve user profiling.

Facebook had to innovate to continue to amass a vast amount of user personal information while appearing to comply with governmental privacy regulations and pressures from civil society. The gamification of its platform and turn towards user-based interaction metadata provided an opportunity for Facebook to amplify its data collection instead of suppressing its practices.

Google developed its advertising network from its Search platform where users performed discreet actions before departing for another destination. Google-based ads had to compete with the limited attention span of users whose objectives were not to view advertising but to complete another task, even if it was commercial in intent. On Facebook, users visit to be entertained. The interaction with Facebook's platform and Google Search is different.

So, the way Google serves ads in sundry products has not changed. Even with Google products that are destinations, the competition for user's attention is against content that users may only browse through quickly.

Previous work on Facebook security mostly focuses on the privacy aspects of the platform and the ever-changing privacy settings (Heyman, De Wolf an Pierson 2014; Lafferman 2012; Hashemi 2009; Milazzo 2014; Johnston and Wilson 2012; Milne and Culnan 2004; Rubinstein and Good 2012). The pervasive nature of surveillance during user interaction with the platform is more serious. Previous work on the commodification of people's attention has not differentiated the long game characteristics of Facebook ads versus the discreet and quick interaction moments that characterize Google's advertising strategy. Previous research (Fuchs 2014) tends to just lump Twitter in with other social media without any differentiation.

My claim about the gamification of privacy and security settings in Facebook take account of the complexity of the architecture and database that enables every user to tag another or block them from tagging him. It is a comprehensive system with many opportunities for data collection. Facebook, as a smart company would be foolish to absorb a low marginal cost for such a complex system without transforming it into a form of potential accumulated capital that can be commodified.

Google is not focused on users' network but more on people's information practices. Google through its apps and services has multiple sites of interaction. Yet it does not attempt to replace or be all the Internet for people the way Facebook tries. Google understands that it is one of many players in the information economy regardless of its size and influence.

While recent developments like Google Now do try to become a part of people's lives, Google knows that it cannot capture every one's attention the way Facebook tries to. For

example, Google is one of two main players in the mobile computing next to Apple. It competes on several levels but does not earn all its capital from advertising.

Twitter is attempting to reconcile security with usability and to profit from the endeavour. Asking users to add personal information and to validate their account strengthen the profiling practices while reinforcing security. Indirectly, the profiling is serviced by usability and user experience practices that seek to offer users an engaged environment where they can pursue their information practices.

Security is not the face of the story when it comes with Facebook. Privacy is the story. The research demonstrates this bias, but Facebook has successfully exploited this perception to its advantage.

Google geared its registration and authentication process towards users who will not stay long. In this moment of interaction, Google must capture a lot of data about users. Hence its data generation and aggregation processes are probably geared towards metadata even though semantic information is also used in its profiling to target users.

While Facebook's privacy policy omits the term 'privacy', registration with the platform leads to the gamified version of privacy settings promoted by the platform. One can infer that Facebook takes the security of the data about users very seriously but does not publicly demonstrate that. This data is everything for Facebook and anything that could corrupt it would challenge its authenticity and the analytic insight the operator derives from its commodification.

The story of Twitter’s risks for users is based on security not privacy. The perception is that privacy is not a concern for Twitter because by default most tweets and exchanges on the platform are public. Security is the problem. As well as hacked accounts, security problems include attacks in the form of trolling (harassment) from some users against other groups. But usability and user experience are also concerns on Twitter as new users find using the platform and engaging with others confusing or overwhelming.

7.2.3 Frame Analysis Discussion

From the frame analysis, I observed that the privacy policies of Facebook, Google, and Twitter do not mention tertiary authentication specifically but make ample mention of third-parties. Although authentication into the platform operators' technology realms is often necessary to access information hosted with them, this act is not the focus of privacy policies. The operators do not frame users' interaction with their platforms. Authentication is like a *fait accompli* necessary and part of the site of interaction with an ephemeral technology. For people's personal data to be collected, the user must be verified. Hence, the ideal starting point of the discussion of what happens to users' personal data is one where the user is authenticated. This happens after users have generated a user token.

Disclosure of third parties' usage of user data is not hidden in the three privacy policies. It happens. However, the trade-off here is between privacy and access as opposed to security and usability. The platform operators are more concerned with making a case as to why people's personal data is necessary in this exchange than discussing potential security risks or usability. Usability here is not the exact value represented by the privacy policies. What is at stake is user experience which encompasses usability and other contextual phenomena unrelated to how users satisfactorily complete tasks. Access to information on the platforms is part of an experience offered to users. Access, as argued in the transactional token framework, is one of the two parts of authentication. But access only occurs if identity verification happens. Privacy as per the transactional token framework, is also one of the property rights that begin to create a space that allows others to identify a person, or the creation of identity. Here, the platform operators do not promise users that they will be able to complete tasks and perform work.

Of the three platforms, Google's services and apps are the most focused on work and productivity. Yet, as mentioned in the policy analysis, Google aims to provide more relevant search results, to help people connect with others, and make sharing fast and easier (2016). The only challenge to Google's objective, which Facebook and Twitter also share, is that addressing privacy is unavoidable. Google appears to act responsibly when addressing it privacy challenge. Twitter informs users about their responsibility when engaging in personal data sharing by using

a legal discourse. Facebook downplays what privacy is and attempts reframe it as a data sharing practice that users manage through a gamified interface.

As argued by Parker (1998) and mentioned in the Policy Analysis, government regulations such as the *Privacy Act of 1974* are the causes of the prevalence of privacy over other information security matters in civil society, and the corporate world. While each platform has well-defined privacy policies, they do not have security policies guaranteeing users that their data will be secured. Security, when mentioned, as seen in the Patreon case, becomes a risk associated with the release of personal data, not integrity, possession, authenticity, or utility. For platform operators, proving their responsibility towards users' security just like they must do with privacy is not as necessary politically, or commercially.

Security remains a potential risk, but platform operators address this problem by shifting the responsibility onto users, requiring them to enter more personal data to perform verifications or encourage them to use enhanced security measures, like two-factor checks when users perform authentication with their platforms. These enhanced security measures often rely with users interacting with technologies at outside sites of interactions which are not present in their current interaction path with the platform.

In this study, I am claiming that privacy is perceived as the main security issue that can affect users. The responsibility for privacy and users' confidentiality appear to be framed as a concern that platform operators control. Similarly, security appears to be framed as a value that users are responsible for. The paradox is that security is a concern that platform operators of the size of Facebook, Google, and Twitter are really concerned about and that can affect their profitability. Privacy and its circumvention through practices such as personal data management, can increase or decrease platform operators' capital accumulation. Authentication, and its tertiary form are not concerns or seen as the first step of the entanglement between security, privacy, usability, and access. This interpretation of the security-usability problem with platform operators and tertiary authentication is a novel interpretation of the problem space. In the next section, I will coalesce these ideas into a response answering the **RQ1**.

7.2.4 Transactional Token Discussion

In the transactional token framework, I contended that privacy and security are overlapping values caught in a dialectical contradictory relationship about who a person is and what a person possesses. When perceived together, these two values reveal much about people's identities as opposed to their humanity. This identity is what is exploited, sought, and commodified by platform operators like Facebook, Google, and Twitter. The documentation of identity happens whether users are logged with one ephemeral technology because platforms can still collect data and exchange it with third-parties. This identity depending on the tracking and the setup of the user's computers, tablets, or phones can be thorough or approximate. Therefore, the concept of ephemeral technologies which argues that people are authenticated at multiple levels of abstraction helps us understand the collection of data for users not logged in directly within a platform. A person using Google Search on an iPad is already authenticated through the device even though she may not be signed in with her Google account as she uses her browser. However, once people generate user tokens, they engage in the first step toward in-session authentication with a primary platform. Identity is verified.

Tertiary and secondary authentication happen when third-party API data is exchanged between third-parties like advertisers or third-party developers and a primary platform like Facebook, Google, or Twitter. However not all tertiary authentications lead to the same type of user data commodification. As argued in the Theoretical Framework chapter, there are many types of tertiary authentications and applications. There is tertiary authentication with data manipulation by a third-party app; tertiary authentication through a cloned third-party app (or client); and tertiary authentication for an unrelated service, app, product that could technically function as a standalone platform. Facebook, Google, and Twitter each support all three forms of tertiary authentication.

Tertiary data manipulation applications use data from primary platforms and can modify or add to it. As well as replacing the primary platforms as clients, these applications can have immense access to user data. They can generate their own data which can be published within the primary platforms or outside of them. Some of the data in this class of tertiary apps must be held in confidence outside of the primary platform. Whether users' interactions with the tertiary

app is recorded as metadata is definite. For example, dlvr.it states in its privacy policy that it does capture data related to users' Internet Protocol address (dlvr.it 2009).

Clones and tertiary clients of primary apps may function as empty shells on a user's computer or mobile device. Short of inspecting the code of each application, it is unclear if some user data is sent to a central server hosted by the tertiary app developer. In such a case such as the Facebook client developed by BlackBerry for the Playbook tablet, data is exchanged between the client app and the device's operating system.

Unrelated services or apps that could function as standalone platforms or games but still use the tertiary authentication through a primary platform like Dropbox may offer their own alternative primary authentication. In the case of a game hosted directly with a primary platform like AngryBirds Friends, they may appear to bypass formal authentication by simply offering a play button feature. Authentication still occurs but it is obfuscated.

7.2.5 Research Question One Report

The interplay (in the form of trade-offs) between security and usability should be understood with timesharing technologies in mind. The marginal capacity cost of hosting people's data includes the intervention, practices, and information systems' controls that must maintain privacy and security features. For example, the marginal capacity cost of maintaining an architecture that allows Linda to block Tommy, and to restrict George's access to only some content of the other two users is embedded in the gamified privacy and security settings on Facebook. Multiplying the interconnections between Linda, Tommy, and George to billions of users allows us to grasp the comprehensiveness of the privacy features at Facebook and why it is in its best interest to exploit the user interaction data produced by people adjusting their privacy and security settings every day.

The settings' console that allows users to adjust their privacy and security settings on Facebook should be somewhat usable and provide some form of satisfactory user experience. This discovery is unexpected. I have not directly tested users' experience when using the privacy and security settings to determine if they have some hedonic quality, yet they are important elements to grasp the trade-offs between usability and security.

The privacy features of Facebook with their gamified interface are proxies for security in the security/usability trade-off. The privacy features serve the interests of Facebook who is attempting to profile its users. The relationships (or failed relationships) between Linda, Tommy, and George offers an immense amount of network data about each user. If Linda's profile lists her as a conservative, a Baptist, and a Republican voter while Tommy, who used to be listed as her cousin tends to repost links to liberal websites, this becomes crucial ways for pre-existing personal data about users to be validated by Facebook. Linda is trying to control Tommy's access to her profile using the privacy settings but her interaction with the privacy settings reveals far more personal information about her identity.

Now George likes to play games on Facebook but although he cannot view all of Linda's and Tommy's posts, he can still chat with them. George's security settings authorize many games that may have been blocked by Tommy but not by Linda. Linda gets an invitation to view and play each game that George plays with. Part of Linda's profile may even be transferred to tertiary game developers. But Tommy has blocked these apps which reveals more about his technological literacy and perhaps even some of his ideological leanings, beliefs, positions on privacy, and ultimately, his education level.

My conclusion about the extent of trade-offs between security and usability when it concerns Facebook is that the platform's operator understands how to render security serviceable to usability to best profile and therefore target users with advertisements. Security, whether directly or through privacy will be exploited as much as possible to better profile Facebook's users. Usability however, becomes a means to facilitate personal data generation, aggregation, profiling, targeting, and ultimately, the commodification of people's information.

Google allows third-party developers to develop apps that connect with its Google+ platform through OAuth 2.0. Google+ accounts are different from the common Google account that can be used by third-party developers to allow users to authenticate in tertiary platforms such as Dropbox. Facebook pursues a similar strategy but also promotes an app ecology that integrates directly into its own platform. Google has a platform where third-parties are invited but it is one that leverages its ubiquitous computing power. Android is the site of interaction for most of Google's third-party developers. Many tertiary apps that integrate with Google products

outside of Android are rudimentary. Business Organizer for Google Docs leverages Google's primary authentication but allows users to perform limited manipulations such as moving a file from one directory to another.

Android tertiary apps are the ones that provide Google with the most user personal data. Stephen, Naomi and Julia each use Android devices for work and for their personal affairs. Stephen uses several devices such as a tablet at home, one at work and an Android phone which all share the same Google account. They have the same apps and even browsing data replicated on each of them. They are really client devices whose information is almost completely held on Google servers and redistributed between the tablets and the phone. These devices are sites of interaction but also have nested sites of interaction in the form of every app that Stephen uses. Moreover, Stephen uses Google Chrome and other services such a Google Docs on his laptop at work and at home. Stephen's Google account links these different sites of interaction together. Google just like Facebook knows which app Stephen installs. Potentially, Google could know the degree of Stephen's interaction with each app.

Some apps like the default Android keyboard app can gather interaction metadata and contents' data if the user allows the monitoring to occur. What is more pernicious is that the default Android keyboard app appears within every tertiary app where users must use a keyboard. The possible data collection is across every tertiary app when the keyboard is present. If Naomi uses an alternative keyboard app from the Android Play store, this app, if the permissions have not been disabled could also record every keyboard entry. Many of the apps that Naomi uses contain advertising that is managed through one of Google's mobile advertising platform like AdMob. AdMob can even mediate other advertising networks' ad repertory.

Julia is a consultant and relies on Google Maps, Contacts and Calendar to schedule meetings on her laptop and to navigate across the city to client's locations. All her locations and travels for the last six years are kept in a longitudinal file in her Google account. Google Maps, Contacts, and Calendar are ad-free but the data they contain about users' interaction with their space, their network and time management is exhaustive. Some of this personal data could be matched with relevant data in the Google sites of interactions that do feature advertising, like Gmail, Search, or YouTube.

Reliance on mobile modalities such as Android devices forces Google to offer very usable sites of interactions but also secured interactions. The Google account and the Android devices are critical spaces that manage a lot of people's everyday lives and activities. Google recognizes this and has reinforced its authentication by offering two-factor authentication and complicated screen authentication schemes for mobile devices. As mentioned above, two-factor authentication encourages users to add sites of interaction and personal information such as secondary email addresses and telephone numbers.

Whereas privacy and security settings in Facebook are gamified experiences set against other users, in Google, these are set against hypothetical enemies who would take over the account and the pervasiveness of Google's data aggregation and generation itself. Even when users delete past personal data collected by Google, the platform will continue to collect more as users interact with various sites of interaction and the third-parties who host Google-mediated advertising.

My conclusion about the extent of trade-offs between security and usability is that Google provides security measures that are framed in the context of usability and user experience to encourage users to become responsible for their security versus a potential unknown risk. Even when Google offers users options to delete their own data it is unclear if the data is removed from the site of interaction that the user sees or if it is eliminated from Google's servers and backups. Because user data is saved on servers across the world, the marginal capacity cost to delete data that users request be eliminated would involve interactions between many various components and information systems. Again, just like in the case of Facebook, it would be in Google's interest to keep metadata about such requests and to use it to better profile and target users.

Security is in the service of usability needs which in turn serve the commodification goals of Google. The extent of the trade-off between security and usability transforms the former (and privacy, as a subcomponent) as features to facilitate the data generation, aggregation, profiling, and targeting of users as they perform authentication whether primary or tertiary. Because of various Google-operated ad networks such as AdMob, AdWords, and the Android mobile platform, tertiary apps and services are constantly interacting with Google either through

authentication or through authorization. The user may not have performed a full authentication while using an ephemeral technology.

Twitter's commodification strategy appears simpler. This strategy competes with Twitter's mission to become an important site for public discourse. Twitter does generate and aggregate data about its users, but this seems to be tacked on as an afterthought to find a way to monetize people's attention. Moreover, Twitter still uses third-party marketers and data aggregators to profile its users. Facebook and Google either buy strategic resources like Atlas (Facebook), DoubleClick[23] (Google), or produce their own solutions.

Having an immature capitalization strategy affects Twitter's usability and user experience practices. Usability and user experience, as reasoned above with Facebook and Google, serve the capital accumulation goals of platform operators. As discussed in the case of Facebook and Google, usability greatly influences security and privacy. With Twitter, what seems more at stake is user retention than the commodification of their personal data and attention. Usability appears to be directed at maintaining Twitter's audience, not benefitting from it directly. For example, Twitter does not feature advertising when viewing a Twitter feed without being authenticated. Only authenticated users are served ads. Facebook does not serve ads to non-authenticated users either but is more vigorous in encouraging visitors to log in.

Privacy matters for Twitter but as mentioned above, it is security and compromised accounts that are part of the narrative of the platform's risks. Security matters more because of the public nature of the information shared by users on Twitter. Although there are ways of communicating privately or limiting one's posts, most information shared on Twitter is public. But the public nature and ease of misrepresentation means that a compromised account could damage the reputation of a person publicly if nefarious tweets were posted by an identity thief. Stolen identities involve both security and privacy. The subterfuge is a security act while the potential result is a privacy risk.

---

[23] DoubleClick is an advertisement aggregator that allows advertisers, and ad buyers to target users based tracked over several websites and platforms. DoubleClick can track targeted uses across domains and platforms.

My conclusion about the extent of trade-offs between security and usability when it concerns Twitter is that usability as part of a strategy of user-retention and audience expansion is a more significant value at Twitter. Security appears in control settings allowing users to remove tertiary apps' access to user accounts, just like with Facebook. However, these settings do not appear to be part of a gamified experience generated by the platform operator. Other measures such as two-factor authentication and the use of personal information to validate an account such as phone numbers appear as part of a strategy to gather more data about users while providing them with security features. Because security is perceived as a greater risk on Twitter than at Facebook, or Google, the management of the security narrative is integrated in the user experience of the interaction design on Twitter. Thus, for Twitter, security serves usability just like with Facebook and Google. But unlike Facebook and Google, security and usability do not yet appear to be part of an extensive process of commodification of people's personal information. Twitter lacks the correct strategy and maturity to monitor ever interaction between users and its platform.

Twitter still relies on user profiling technology from Google Analytics and other third-party providers. It has not demonstrated the maturity or the expertise to control every interaction on its platform to the extent that Facebook and Google do. As for some of its security features, Twitter still relies on a questionable implementation of OAuth which provides tertiary with unlimited access tokens that do not expire (Hammer-Lahav 2010). This lack of expiration could be interpreted as a security risk as there is no limit to how long a tertiary app or service can access user data. However, OAuth 1.0 (and 1.0a) still require third-party developers to use encryption processes and has limited support with non-browser-based access requests from tertiary apps and services (Hammer-Lahav 2010).

Developing tertiary authentication for Twitter is significantly more difficult than developing similar processes for Facebook or Google. OAuth 2.0 is more usable for developers meaning that tertiary app development is less efficient with the former. This can impact the total tertiary app development of Twitter, which affects the potential platform operator's gains with tertiary authentication and users' personal data commodification. Hence Twitter does not appear to rely much on tertiary authentication to further commodify the attention or interaction of its

users with third-parties. Unlike Facebook and Google, Twitter seems to want to maximize data generation and aggregation directly within its platform.

User experiments such as AB testing are meant to improve usability and user experience to improve how users interact with the platforms or to funnel their interactions in one path or another. More than Facebook and Google, Twitter appears to suffer from scarcity and struggles with its marginal costs.

7.3 The Experimental Background and Motivation

The quasi-experiment had three conjectures which collectively help me answer research question 2 and 3. **RQ2** asks how people are performing tertiary authentications as they manage and control their security and confidentiality and what are the implications of those actions for users' perception of identity and privacy. **RQ3** asks which conditions and variables create a perception of false security in users performing tertiary authentications and what factors of tertiary authentication affect users' sense of security.

Conjecture 1 which was concerned with participants' mental models and how they differ from the design models used by platform operators was tested with the diagrammatic mental model representations that participants had to draw after each task during the quasi-experiment. Conjecture 2 tested if users rated the value of their profile moderately to strongly when told that their personal information was not editable or removable when performing tertiary authentication. Lastly, Conjecture 3 tested if participants would selectively restrict access to their profiles with third-party apps if they the option to do so.

7.3.1 Closed-Ended Answers

The result of every Likert questions from the questionnaire was inconclusive with a retention of the null conjecture. While the Likert questions used in the quasi-experiment did not successfully test **C2** and **C3**, they did elicit interesting data that can support the inquiries raised by **RQ2** and **RQ3**.

7.3.1.1 Conjecture 2

Conjecture 2 measured user control and management of personal information during tertiary authentication. The independent variable for **C2** was participants' explicit knowledge that the personal information shared by primary platforms with third-parties' apps are neither editable nor removable (by asking them to adjust their security and privacy settings in Facebook, Google, and Twitter). The dependent variable for **C2** was participants' selective restriction of third party apps access to their profile.

There was no covariation found between asking the test participants to adjust their accounts' security and privacy settings and whether they would selectively restrict access to their profiles when performing tertiary authentications. The Likert scale questions could not prove a relationship because of internal validity challenges.

In the pre-tasks, participants had to adjust their Facebook, Google, and Twitter settings to enable tertiary apps to be installed through tertiary authentication. Without this, the quasi-experiment could not be performed successfully. Because of privacy and ethical considerations, participants had to perform the changes to their accounts, following instructions from the study's investigators. This step is like the one where test participants had to change their security and privacy settings. This may have created a confounding variable for all participants, including those in the control group. This would have created challenges with the internal validity of the test.

The questions asked for **C2** are directly related to the dependent variable which was about participants restricting access to their profiles when performing tertiary authentication. However, the questions did not test the independent variable directly. A Likert scale questionnaire may not have been sufficient to measure the relationship. Instead, observation of how users reset their accounts during the post-task would have been more appropriated. My research assistants and I did notice and took notes about which apps participants kept or removed access to during the post-task with Facebook and Twitter. There were no equivalent procedures with Google. Some participants kept some tertiary apps' access and disabled others. Because of privacy and ethical considerations, we could not directly observe or record which apps

participants kept. We did ask participants about which app and service they kept but it was not requested systematically. Even if we had, we could not use this nor records or observation to test **C2**'s validity with Google.

7.3.1.2 Conjecture 3

Conjecture 3 measured how users rate the security of their personal information when aware that it is not editable or removable while performing tertiary authentication and shared with third-parties. The independent variable for **C3** was participants' explicit knowledge of what personal information platform operators share during tertiary authentication processes (by reading a privacy, security an data policy documents from Facebook, Google, and Twitter). The dependent variable for **C3** was participants' selective restriction of third party apps access to their profile.

There was no covariation found between asking the test participants to read a user agreement and a privacy policy for each platform and the rating of the value of their profile when comparing them against the control group. It appears that reading a user agreement, or a privacy policy is a practice without enough causality to affect how participants value their profiles. One can infer that this is a normalized practice among users in general and part of people's everyday practices.

The Likert scale questions could not prove a relationship because they did not ask direct questions that would test if reading a user agreement and privacy policy for each platform affected how participants valued their profiles. **Table 35** contains questions that would have drawn a tighter relationship between the variables tested with Conjecture 2.

Table 35 - Alternate Conjecture 3 Testing Questions

Qa	I value my account so I take every step to protect it by informing myself by reading user agreements and privacy policies when using a platform Facebook, Google, or Twitter.
	[Never Rarely Sometimes Often Always]
Qb	Reading Facebook, Google, and Twitter's user agreements will help protect the value of my account with these platforms?
	[Strongly Disagree Disagree Neutral Agree Strongly Agree]

Qc	Users who do not read user agreements and privacy policies do not care about their security and privacy of their accounts.
	[Strongly Disagree Disagree Neutral Agree Strongly Agree]
Qd	User agreements and privacy policies protect people's accounts.
	[Strongly Disagree Disagree Neutral Agree Strongly Agree]
Qe	User agreements and privacy policies can protect my account from third-party apps and services which I access through Facebook, Google, and Twitter.
	[Strongly Disagree Disagree Neutral Agree Strongly Agree]
Qf	My Facebook, Google, and Twitter accounts are important parts of my identity.
	[Strongly Disagree Disagree Neutral Agree Strongly Agree]

Instead, the questions used for **C3** provided elicitation better suited for answering the second part of **RQ2** which asks about the implications for users' perception of identity and privacy when they manage and control their security and confidentiality as they perform tertiary authentications.

The questions used in the quasi-experiment tested participants' existing conditions, perceptions, and practices related to security, confidentiality, usability, and privacy. These conditions, perceptions, and practices may not have been affected sufficiently by the independent variable which required the test group to read user agreements and privacy policies. The questions asked for **C3** tested participants' information literacy with social media and were not reliable enough to obtain statistical validity for the conjecture.

The random heterogeneity of the participants (Cook and Campbell 1979, 44), due to their information literacy prevented the test from providing a valid outcome based on the questions. Reading (or avoiding) a user agreement and a privacy policy appear to be common acts that do not sufficiently create covariation with how participants' value their profiles. In the context of the study, as part of the ethics' procedures, the study's investigators had to summarize verbally the study's contract which mentioned privacy and security aspects related to the study although I had attempted to control for their influence at the research design stage. It is possible that reading the consent form aloud and making the participant aware of it created a confounding variable that affected the efficacy of the experimental test for **C3**.

7.3.2 Conjecture 1: Mental and Design Models

This section discusses the results of **C1** measures user control and management of personal information during tertiary authentication. I conclude that **C1** is valid based on the diversity of mental model representations from participants in the study.

As argued by HCI psychologist Robert Hockey (1990), users' mental models must be understood as representations generated by a mix of competences and control skills related to how people process information. Hockey defined competence as a basic information processing property. He defines control as the skills required to manipulating and managing cognitive resources. Hence every participant in the study has different levels of skills and abilities when they rendered their mental models using the diagrammatic elicitation. The measurement of participants' cognitive skills and abilities is not an objective of this study. As HCI scholar Thomas Green (1990) claims, it is often sufficient for HCI research in people's mental models to limit itself to understanding representation schema without having to clarify cognitive processes, such as working memory which are best explain by the cognitive sciences (Green 1990).

Regardless of the cognitive processes that influenced users' diagrammatic elicitations, it can be argued that each representation being so different from one another render null any standardized mental model that could then be matched to a hypothetical design model provided by Facebook, Google, and Twitter. In this study, I did not seek any design models from platform operators because of the complexity and time-limit needed. Only if all three platform operators provided schematics resembling a unified design model could their contribution be used as points of comparison with participants' diagrams. The shape of such design model could have differed from the diagrammatic elicitation form used in this study. Worse, little common ground would probably have been found between the operators' design models that could successfully be translated into a useful and usable form for this study. Lastly, it would have been impossible to use a design model that could depict the interactions with the mix of tertiary and secondary apps and services used in this study without significant editing of original documents provided by Facebook, Google, and Twitter.

The closest design model that could be used as a comparison to participants' diagrammatic elicitations were the instructions we read during the quasi-experiment. The instructions were delivered orally by the same investigator and had the advantage of being optimized for each task participants performed. Still participants demonstrated a wide range of variety in their diagrams when it came to describe their perceptions about tertiary authentication.

Specific examples of divergence between participants' mental models' representations and operators' design models are easy to identify even without having de facto documentation from Facebook, Google, and Twitter. For example, as seen in **Table 58**, a minority of participants did not represent the login step in their diagrams. The only task where all participants represented a login was with Dropbox. Moreover, as discussed in the Experimental Results, some participants depicted the primary platform as preceding the tertiary app in the tertiary authentication process. For these users, they started the authentication process by using Facebook, Google, or Twitter first and only when they logged in did they start using the tertiary app or services.

Even when following step by step instructions, participants demonstrated their agency in the representation of their mental models that explained how they performed tertiary authentication.

7.4 Research Question Three: Answer

I chose to answer **RQ3** ahead of **RQ2** because exposing the answers to this question will allow me to respond fully to the latter. In **RQ2**, I will combine elements from both research question 1 and 2, as well as **C1** to respond to the question asked. **RQ3** asked about which conditions and variables create a perception of false security in users performing tertiary authentications, and what factors of tertiary authentication affect users' sense of security. Several conditions and variables create a perception of false security in users performing tertiary authentications. Some of these conditions and variables are limited postings on primary platforms and tertiary apps, including how much and what is posted, control over the place where interactions happen, using known devices, and password management practices.

7.4.1 Limited Postings

Participants indicated that they make decisions about what they post and how often to control the personal information that is held by primary platforms and that potentially could be distributed to tertiary apps operators, or marketers. **P18** wrote *"...because I am a private person and sometimes I do not want a circle of social network from one account view my things off another account.*" **P16** commented that "*I usually limit my exposure and access of personal postings to myself and friends.*" **P12** shared a familiar trope writing "*Don't post anything you wouldn't want your mother or employer to see.*"

As argued above, metadata based on users' interaction may still be collected and can still reveal personal information about people. This information is collected through the devices users use and through their behaviour on platforms. Limited postings only control for semantic information sharing.

7.4.2 Using Known Devices

Using known and safe devices is one strategy that participants employ, and this provides a false sense of security when performing tertiary authentication. **P09** wrote *"...I also verify the devices that are currently logged in.*" This practice is also used by **P14** who writes "*Only logging in via hardware I know is from a safe source.*" **P19** suggests *"... [to] always logout and delete cookies /cache after using public computer.*"

While this practice has merit, it only provides security from external threats and possible risks such as other users sharing the same devices. Just like users who attempt to control their place of interaction, this practice only affords security over potential risks and not those that may come from tertiary app and service developers whose servers could be compromised even if they have the best intentions for their users.

7.4.3 Control over Place of Interaction

The control over the place of interaction is related to all forms of authentication and not the tertiary type. For some participants, where they interact with an information system seems relevant enough to provide security about while performing tertiary authentication. **P02** wrote

"*When I loggin o my account in public I am more catious (sic).*" P20 wrote *"...Be sure that no one is looking at you meanwhile you are signing in...*"

It is interesting that for such users, security risks come from an unknown other that could be lurking near them in public. It is a similar fear that affect people withdrawing money from bank machines or using their credit cards in stores. Information security risks become potential risks borne out of our practices in the information economy. This is a perspective, which I have argued repeatedly in this research that match the risk society theory argued by Beck about post-modern human-made societal threats. I argue that information security should be added to the list of threats that people in the information economy face. Environmental collapse, pandemics, economic collapse, and terrorism are similar threats.

7.4.4 Password Management Practices.

Password management practices are the richest and most varied solution to security participants rely on when performing tertiary authentications. **P01** suggests the "*use [of] separate passwords for each platform and select carefully which 3rd party apps to allow access to those platforms.*" **P03** used a common advice which is to "*use complicated passwords no one can easily guess.*" **P20** proposes changing passwords every 90 days.

As argued by Adams and Sasse (1999), changing passwords frequently does not provide more security if users must memorize new schema frequently. Users may favour simpler passwords that can increase their vulnerability (Adams and Sasse 1999). Using multiple passwords for different venues or complicated schema, also reduce memorability and can encourage users to write them down in a non-secure place (Adams and Sasse 1999). The point of my criticism of participants' suggested solutions is not to belittle them but to note the low level of literacy that can contribute to a sense of false security when they perform tertiary authentications.

Tertiary authentication factors that affect users' sense of security are usability, modalities and sites of interaction, clone clients, tertiary apps, and security and privacy settings. Factors that affect users' sense of security may not be visible or known to users. While independent variables in the classic experimental sense, these factors are not practices or discreet conditions even

though they can be reduced as such if controlling specifically for one instance. For example, two-factor authentication can be a discreet expression of modalities of interaction.

7.4.5 Usability

Usability is an important impetus for tertiary authentication as it reduces the number of passwords users must recall when interacting with multiple sites of interaction. **P16** confirms this by writing "*Logging onto third-party apps via Facebook, Twitter or Google allowed for a very convenient & streamlined process without having to register for a new account. It is more convenient on the laptop than other tablets due to the interface.*" Tertiary authentication processes also reinforce common mental models in users' minds. **P01** wrote "*Most apps seemed to use the same language to explain I was using Facebook/Google/Twitter to create accounts.*"

An issue with tertiary authentication and usability is what happens once the user has logged in and the tertiary app start controlling the flow of interaction. This is not something that primary platforms can control, and it may affect the usability advantage established with tertiary authentication. As **P13** writes "*Sometimes logins took place over multiple screens, other times all actions occurred on a single screen. Some apps imported usernames, other had me enter everything from scratch.*" **P14** added "*Yes. Some apps were much more streamlined and allowed for quick access while others were quite convoluted with supplementary ad ons.*" For some participants, there were little usability benefits to using tertiary authentication. As **P11** wrote "*Visual cues were different; Messages given by platform/app different; No clarity as to what info crosses over; No clarity as to why it is more convenient [.]*"

7.4.6 Modalities and Sites of Interaction

Modalities and sites of interaction greatly affected participants' sense of security. Here, I argue that modalities and sites of interaction are codependent variables that affect users' sense of security as they perform tertiary authentications. **P10** appears to claim that sites of interaction matter more than modalities by writing "*Log in was easier on laptop & iPad since I am familiar, but liked logging in on Android – flowed nicely. I did not like apps that overwhelmed with log in options [.]*" Here, it appears to be the site of interaction that determines how usable the tertiary authentication is. However, how users interact with the laptop, the iPad, and the Android tablets

is through modalities of interactions. As **P12** wrote "*It's harder to login with tablets because of the touchscreen keyboard.*"

The link between modalities and sites of interaction can be difficult to observe. For example, **P20** writes "*Sometimes I prefer to use some apps in the computer and other ones in the tablets; it's only something visual. When I logged into each platform, everything was fine.*" Modalities are the means through which users interact with sites of authentication beyond reading static screens. Every decision they make, especially with tablets involves modalities such as gestures and taps.

A way to understand the relationship between modalities and sites of interaction when it comes to tertiary authentication is to look at two-factor authentication. Two-factor authentication occurs on several sites of interaction such as laptops, tablets or mobile phones. **P09** experienced difficulties using two-factor authentication on several sites of interaction, writing "*Yes, I had 2-step authentication that was causing difficulties, especially with Google on receiving code on the phone.*"

In the Experimental Findings Chapter, I observed that modalities of interaction are not always in participants' mental models' representations. As argued there, this is related to participants' idiosyncratic ways of representing their mental models as opposed to something that may be influenced by their perceptions of security and privacy. However, the placement of their tertiary authentication process in the diagrams reveals a lot more about how people perceive tertiary authentication.

7.4.7 Clone Clients

Cloned clients such as Facebook for the BlackBerry Playbook cannot easily be differentiated by participants as noted in the diagrammatic coding of the Experimental Results Chapter. Ninety percent of participants did not indicate any relationship between the Facebook app for the Playbook and Facebook as a primary platform. BlackBerry did design this app to mimic and offer a complete 2011 Facebook experience when the platform operator did not release an app for that platform (Boulton 2011). It was a similar situation with Palm's webOS platform the same year (Schonfeld 2011).

While with high-literacy users can probably differentiate official primary apps from tertiary clients, it is not a truism for most people. This can create security problems, especially when users rely on third-party clients as proxies when they interact with primary apps. Both BlackBerry and Palm released their Facebook apps as semi-official clients when Facebook refused to produce its own clients for these mobile device manufacturers and their mobile operating systems (Boulton 2011; Schnofeld 2011). Instead, Facebook offered access to its APIs which allowed both manufacturers to develop clients that mimicked the primary platform as much as possible.

Facebook discontinued support and removed access to its APIs for the webOS Facebook app in 2015 (Hunter 2015). The effect was immediate on current and past users of webOS devices. All the posts and pictures that they had uploaded with their webOS devices were hidden by Facebook and no longer accessible (Hunter 2015). Although Facebook eventually relinked the lost data to users' accounts, this case exhibited Parkerian security problems related to availability and possession. For a period of four months, the webOS-generated data was no longer available on Facebook even though it had not been deleted (Hunter 2015). It also raises a question about the possession and control of the data by users. Facebook chose to remove access to user-generated personal data that had been upload through webOS devices.

When the data was made available again, Facebook chose to remove tags noting the origin of the data from 'Facebook for HP webOS' (Hunter 2015). While a minor change, it does raise other Parkerian security questions related to integrity and authenticity. The tag 'Facebook for HP webOS' was metadata attached to the actual contents. Yet its removal makes it appear that webOS users uploaded the data through the Facebook primary app. It makes the authenticity of the data somewhat less authentic as it was not generated through Facebook. Facebook similarly removed support to its API for the Facebook app for BlackBerry Playbook in 2016 creating interoperability with the device and the primary platform (Statt 2016).

As noted in the policy analysis, Twitter has also limited the access to its APIs to developers making Twitter clients. In cases such as that of MetroTwit, a popular Twitter client for Windows computers, once the Twitter imposed limit of 400,000 has been reached, new users can no longer download or use the app (Warren 2014). This may not appear as a direct security

risk to users as it affects developers. Yet, the risk of having no more access to the client app is real.

7.4.8 Tertiary Apps

Clone clients are but one type of tertiary app where users can struggle for the control of their personal information once they have allowed access to their primary platform's accounts. Some users have legitimate concerns about the data exchanged between primary platforms and tertiary apps. **P01** writes "*I have concerns as much of my personal information is on those platforms, and it wasn't clear how much was being shared with the 3rd party app (i.e. was only my email being shared or was the content of my emails also shared?)*" To alleviate their concerns with determining if a tertiary app is safe or not, some participants rely on recommendations and reviews from the primary platform's app catalog. **P15** writes "*Make sure the app using the platform has been suggested by platform I trust.*" In terms of control over data after their primary accounts have been deleted many participants displayed a sign of resignation over their perceived lack of control over their personal information with tertiary apps. P5 writes "*They will still have the information on 3rd party appys (sic).*" **P10** is blunter by writing "*They probably keep it.*" Again, control over personal information held by tertiary apps echoes my arguments about how information security concerns is now part of Beck's risk society.

7.4.9 Security and Privacy Settings

Security and privacy settings appear to be the solution that platform operators offer their users to alleviate their fear of risk with their personal information. These features appear to be usable for many users and to offer people just enough security and control over privacy. **P14** writes "*...It makes it very easy. My concern is always w/ the apps posting to my page w/o consent but I can see there are settings to disable that.*"

Twenty-five percent of participants listed adjustments to their security and privacy settings as measures they use to remain secure on Facebook, Google, and Twitter. Forty percent would suggest to acquaintances adjustments to their security and privacy settings as measures to remain safe. However as argued for **RQ1** and above, adjusting security and privacy settings only

control for potential risks with unknown threats but do not protect users from the platform operators.

7.5 Research Question Two: Answer

I left **RQ2** for last because answering this question last allows me to pull arguments from all previous questions and conjectures and craft a response that reflects the full scope of this study. The first part of **RQ2** asks how are people managing and controlling their security and confidentiality as they perform tertiary authentications and what are the implications of those actions for users' perception of identity and privacy. Tertiary authentication relies on password-based authentication schemes used within federated authentication processes. The primary authentication performed with Facebook, Google, and Twitter is password-based and may even use other schemes such as password managers or paper tokens allowing the user to input their secret token. Once the authentication with the primary app has been completed, the tertiary app requests access to the user's account and uses this as the basis of its own identity verification. This is the federated part of tertiary authentication.

Participants in this study relied on common password protection schemes like two-factor authentication; adjusting their security and privacy settings; changing passwords frequently; or made their password very complex or unique. They also attempted to control for the place of interaction where they used their passwords, to control for the devices that they use, and to clear metadata such as cookies left behind on such devices. Participants also read some of the privacy and security policies associated with platforms, apps, and services. They attempted to verify the reputation of apps that they installed and control for access rights requested by third parties. Other strategies involved self-censorship by limiting the amount and nature of the information shared with primary platforms.

Participants use as series of practices that seem 'right' and sufficient to offer them proper security and to some extent confidentiality and privacy when dealing with other users that may be part of the platforms or not. Their prevention practices also protected them from onlookers in public places or other people that could have access to the same devices that they use. However, little of these practices protect users from platforms and the threats that may affect large sites of

interaction like Facebook, Google, and Twitter. Moreover, when participants perform tertiary authentications they do not manage their security and confidentiality towards primary platform operators who may begin commodifying their personal information.

This situation leads into the second part of **RQ2**. What are the implications of those actions for users' perception of identity and privacy? Based on participants' security practices when performing tertiary authentication, I argue that participants perceive that they have little agency over their identity and privacy but attempt to strengthen and secure themselves the best way that they can. They may like **P11** they may *"[s]et account higher security level.*" Or as **P14** writes "*Less is more and don't go crazy – always be cautious when posting/sharing/sending.*" They may also feel nihilistic and just assume as **P10** that "*[n]othing is that safe…*" and thus not interacting with any primary platform is the solution.

Disengagement from social media and other web-based technology, as argued by digital media scholar Ben Light (2014) is part of a continuum with appropriation. Disengagement from social media, he argues must be understood as a process that also means engagement (Light 2014). Users, based on perceived power relations with primary platforms can choose how much they push or pull from Facebook, Google, and Twitter. Practices such as liking a post, tagging a user in a picture, blocking a former friend, setting up privacy and security settings, Light argues, are part of a constant back and forth between appropriation and disconnection (2014).

Light (2014, 124) suggests that Goffman's theory of personal presentation with front stage and backstage personas are at play and can be used to explain the appropriation to disconnection continuum he advances on his work on people's disconnection from social media. As argued in the theoretical chapter when discussing the contribution of Goffman to this study, tertiary authentication is an example of the transformation of interactions into value exchanges in the information economy. While people decide the extent of their interaction with Facebook, Google, Twitter, and tertiary apps, the operators of those primary platforms must bear marginal operating and capacity costs incurred when acquiring new users and maintaining and securing existing data on their servers.

Users shift and change their perceptions of identity and privacy based on how much information they have about the other party interacting with them at any given moment. Just like **P12** who probably perceived the Facebook for the BlackBerry Playbook as being produced and thus allowed it full access to her account blocked Spark, the email client that sought access to her emails. Then, she allowed Hootsuite and Talon from accessing her Twitter account while blocking dlvr.it requests to access her Facebook account.

However, little of this play and security posturing helps users navigate the metadata and behavioural tracking they generate even as they set their security and privacy settings to protect themselves from potential risks in the form of other users, hackers, and criminals. Facebook, Google, and Twitter continue to collect data on users regardless of their levels of engagement or disengagement with their platforms, provided authentication has been performed. The commodification of personal data generated through tertiary authentication can continue and even benefit from the security practices people engage with.

The implications for user's perceptions of identity and privacy are that if people believe that their level of engagement or disengagement with primary platforms and tertiary authentication, while securing their personal information held in confidence protects them that they will continue to play back and forth with and provide valuable metadata that can be collected by Facebook, Google, and Twitter. The first potential risk are primary platform operators that commodify people's personal information and offer no reprieve to users once they are authenticated. The second potential risk are the security practices of primary platform operators and third-party developers. The third and most pressing potential risk for people's information is the OAuth infrastructure that makes the current tertiary authentication schema possible.

Chapter 8
Conclusion

In this study, I sought to explain people's perceptions of security and confidentiality as they performed tertiary authentication with Facebook, Google, and Twitter. This study is positioned within the human-computer interaction aspects of information studies. Specifically, this study explored authentication, a core component of usable security, itself an area of expertise within HCI. This study also tackled information policy, another core focus area within information studies. An important methodological contribution of this study has been the use of experimental methods with a social sciences-based inquiry. While social scientists use experimental methods frequently, previous studies tend to rely on observation, interviews, and ethnographic methods more than experimental ones.

While only Conjecture 1 of the quasi-experiment yields conclusive results, the data gathered for Conjectures 2 and 3 helped me orient and defend the three research questions of this project. In fact, only part of the data collected in this study was used in the analysis. Much of the data pertaining to primary and secondary authentication was not analyzed or used. This data, when combined with other insights from the current study will allow me to pursue many studies in the future that pertain to tertiary authentication and the commodification of users' data through gamified security and privacy settings.

8.1 Contributions

8.1.1 Diagrammatic Representation of Mental Models and HCI Research

Mental model research is an evolving avenue of human-computer interaction scholarship. Mental model research was introduced from psychology to HCI by Don Norman (1983, b). Unlike Johnson-Laird who used this theory of the mind to analyze various ideas and phenomena, in HCI, mental models are focused on how people understand technologies (Sasse 1997). This distinction matters as described by computer scientist Angela Sasse (1997), whose dissertation studied the description and elicitation mental models from people. She argues that in mental models representation techniques, the mode of representation often used is picture-like, or visual, instead of language-based.

Although Sasse's research highlighted the contribution of mental models to HCI research the scope of original contribution has not grown as much beyond the work of Norman and Laird-Johnson. The visual constraints of the representation of mental models are known but the richness of visual architecture seems to not have caught the attention of the HCI community. The diagrammatic representational method used in this dissertation goes beyond much of the work on HCI and mental models. Perhaps because of my bias as a cartoonist, I understand that the representation of mental models through illustrations or diagrams is not something simple. The method proposed here is well-grounded theoretically, tested and flexible enough to capture the brevity of mental models that flow through people's minds.

8.1.2 Transactional Token and Commodity Theory

The transactional token framework introduced in this dissertation diverges from the main body of work produced after Dallas Smythe's original contribution. There was a need for a theory that explained the process of commodification that occurs when people interact with information technologies that looked at all the mechanics of commodification as they happen. Using Clark's control point analysis was one of the best ways to step away from the macro-critical approaches that blame engineers, marketers, companies, and systems without ever explaining what happens in greater detail. Outside of platform studies scholarship (Dijck 2009; Dijck and Nieborg 2009; Gerlitz and Helmond 2013; Kennedy, Poell and Dijck 2013; Srnicek 2017a; Srnicek 2017b), Fuchs (2012) has come closest to criticizing commodification processes in the social networks but leaves large gaps unaddressed. Some of those gaps are related to how users interact with technology.

In this dissertation, I have argued, as Paul Dourish (2001)did, that the contextual and interaction approaches matter as much as the linguistic and verbal way people gather information. So instead of focusing on the traditional political economic critique of capital, I focused on the other side of political economy, namely the economics. By using well-known theorems such as marginal costs and scarcity, I consider the perspective of platform operators to determine why commodification is deemed necessary.

8.1.3 Usable Security - Authentication and Privacy

Authentication as described in the literature review is one of the most popular areas of research in usable security. The other is privacy. Privacy research in usable security feels awkward as it introduces a social science topic in a community of practice that often sees itself as an empirically-based community. The focus on privacy is so important that scholars in the community have labeled the major conference (Symposium On Usable Privacy and Security – SOUPS) in the discipline **usable privacy and security** (The ACM Digital Library 2018). But the traditions of research on privacy stemming from social sciences may appear odd in usable security research. One can imagine with difficultly Christian Fuchs attending and speaking at a usable security proceeding. Bruce Schneier may be one of few researchers who bridges both the critical and critical divide. In this research, I have done just that by demonstrating that critical approaches from social sciences and others, such as economic theories have their place in studies about how people interact with technologies. And the best part is that it also reunited the two main strands of usable security research – authentication and privacy, in one project.

8.1.4 Critical HCI

Much of the research that studies how people interact with technology from social scientific perspectives comes from science and technology studies (STS). This research community is close to HCI yet macroscopic perspectives are favoured in STS. This posits that while case studies are of interest to STS researchers, they are not always granular. Communities of technology users and developers may be studied but rarely are they tested with experimental methods. Deductive approaches are more prevalent than inductive ones. The site of study based on the individual user is rarely of interest in STS, except in studies relying on ethnography.

Suchman (2007) and Dourish (2001) whose scholarship is not always accepted as belonging to HCI are some of the few researchers in that discipline close to critical traditions. Instead, criticisms about HCI scholars being too instrumental prevail. But HCI can answer many critical questions that involve how people use technology and what are the consequences of users' practices on structures such as platforms that provide them with sites of interaction. It is my wish to have contributed significantly to critical approaches in human-computer interaction research in this dissertation.

8.1.5 The Risk Society and Information Security

The internet and mobile technologies were not widely spread and nearly ubiquitous when Beck wrote *The Risk Society* (1992; 2002*)*. Beck formulated his theory on understandings from 1980s scholars that we were clearly beyond the modern age and into the information economy or what others have termed, postmodernism (Beniger 1986). Nevertheless, the password and other forms of authentication really matter and are part of the risk society. Authentication is an aspect of information security which I have advanced should be part of studies of a risk society just like epidemics, economic mayhems, and environmental disasters. More than the other types of postmodern risks, information security risks such as viruses, identity theft, or phishing, are totally man-made.

8.2 Future Research

Using the insights and knowledge gained in this dissertation here are the areas of research that I want to pursue in the future as a critical HCI and usable security scholar.

a) First, I want to test the perceptual analysis used in the policy analysis in an experiment with participants. It will appear obvious to readers that such a study would have cemented many of the arguments advanced by one lonely scientist;
b) Then, I want to perform more testing of tertiary authentication with newer questions and observe how users adjust privacy and security settings after being asked to do it in an experiment;
c) Next, I want to continue testing users' security and confidentiality perceptions of tertiary authentication but with larger number of users to provide stronger empirical grounding. One limitation in this study which used a traditional number of users for an HCI experiment, was the difficulty in recruiting candidates that had limited exposure to the tertiary apps tested. The difficulty will only increase as tertiary authentication becomes a common practice;
d) I want to perform more research with the diagrammatic representation of mental models I created.
e) Finally, more research needs to be done to unearth how Facebook, Google, and Twitter collect user metadata and how it is used. Perhaps getting them to admit this practice so

that users could control how data collected and their interactions are monitored by platform operators.

References

Ackerman, Mark S., and Scott D. Mainwaring. 2005. "Privacy Issues and Human-Computer Interaction." In *Security and Usability: Designing Secure Systems that People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, 381-399. Sebastapol: O'Reilly.

Ackermann, David, and Thomas Greutmann. 1990. "Experimental Reconstruction and Simulation of Mental Models." In *Mental Models and Human-Computer Interaction 1*, edited by David Ackermann and Michael J. Tauber, 136-150. Amsterdam: North-Holland.

Adams, Anne, and Martina Angela Sasse. 1999. "Users Are Not the Enemy." *Communications of the ACM* 42 (12): 40-46.

Albert, William, and Thomas Tullis. 2013. *Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics.* 2nd Edition. Amsterdam: Morgan Kaufmann.

Amalberti, R. 2001. "The paradoxes of almost totally safe transportation systems." *Safety Science* 37 (1-2): 109-126.

Andrejevic, Marc. 2013. *Infoglut: How Too Much Information Is Changing the Way We Think and Know.* New York: Routledge.

—. 2007. *iSpy: Surveillance and Power in the Interactive Era.* Lawrence: University Press of Kansas.

Andrejevic, Mark. 2014. ""Free Lunch" in the Digital Era: Organization Is the New Content." In *The Audience Commodity in the Digital Age*, edited by Lee McGuigan and Vincent Manzerolle, 193-206. New York: Peter Lang Publishing.

Andress, Jason. 2011. *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.* Waltham, Massachusetts: Syngress.

Arthur, Christopher J. 2002. *The New Dialectic and Marx's Capital.* Leinden: Brill.

Barocas, Solon, and Helen Nissenbaum. 2014. "Big Data's End Run Around Procedural Privacy Protections: Recognizing the inherent limitations of consent and anonymity." *Communications of the ACM* 57 (11): 31-33.

Bates, Benjamin J. 1988. "Information as an Econimic Good: Sources of Individual Scial Value." In *The Political Economy of Information*, edited by Vincent Mosco and Janet Wasco, 76-94. Madison: The University of Madison Press.

Bechmann, Anja. 2014. "Non-informed Consent Cultures: Privacy Policies and App Contracts on Facebook." *Journal of Media Business Studies* 11 (1): 21-38.

Beck, Ulrich. 2000. "Risk Society Revisited: Theory, Politics and Research Programmes." In *The Risk Society and Beyond: Critical Issues for Social Theory*, edited by Barbara Adam, Ulrich Beck and Joost Van Loon, 211-229. London: Sage.

—. 1992. *Risk Society: Towards a New Mordernity.* Translated by Mark Ritter. London: Sage.

Beniger, James R. 1986. *The Control Revolution: Technological and Economic Origins of the Information Society.* Cambridge, Massachusetts: Harvard University Press.

Berg, Tessa, and Rob Pooley. 2013. "Contemporary Iconography for Rich Picture Construction." *Systems Research and Behavioral Science* (30): 31-42.

Bergvall-Kåreborn, Birgitta, and Debra Howcroft. 2013. "'The future's bright, the future's mobile': a study of Apple and Google mobile application developers." *Work, employment and society* 27 (6): 964–981.

Bergvall-Kåreborn, Birgitta, and Debra Howcroft. 2014. "Persistent problems and practices in information systems development: a study of mobile applications development and distribution." *Information Systems Journal* 24: 425–444.

Bermejo, Fernando. 2009. "Audience manufacture in historical perspective: from broadcasting to Google." *New Media & Society* 11 (1&2): 133-154.

Bhatia, Jaspreet, Travis D. Breaux, and Florian Schaub. 2016. "Mining Privacy Goals from Privacy Policies Using Hybridized Task Recomposition." *ACM Transactions on Software Engineering and Methodology* 25 (3): 22:1- 22:24.

Bonneau, Joseph, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes." *2012 IEEE Symposium on Security and Privacy.* San Francisco: IEEE. 553 - 567.

Bonnici, Laurie J., Manimegalai M. Subramaniam, and Kathleen Burnett. 2009. "Everything Old Is New Again: The Evolution of Library and Information Science Education from LIS to iField." *Jpurnal of Education for Library and Information Science* 50 (4): 263-274.

Borra, Erik, and Bernhard Rieder. 2014. "Programmed method: developing a toolset for capturing and analyzing tweets." *Aslib Journal of Information Management* 66 (3): 262-278.

Boulton, Clint. 2011. *RIM PlayBook Gets Video Chat, Facebook Apps.* May 2. Accessed April 30, 2017. http://www.eweek.com/pc-hardware/rim-playbook-gets-video-chat-facebook-apps.

Brügger, Niels. 2015. "A Brief History of Facebook as a Media Text: The Development of an Empty Structure." *First Monday* 20 (5). Accessed September 27, 2017. doi:http://dx.doi.org/10.5210/fm.v20i5.5423.

Brunk, Benjamin. 2005. "A User-Centric Privacy Space Framework." In *Security and Usability: Designing Secure Systems that People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, 401-420. Sebastapol: O'Reilly.

Burke, Edmund. 1990. In *Miscellaneous Writings*, edited by E. J. Payne. Indianapolis, Indiana: Library of Economics and Liberty. Accessed March 6, 2017. http://www.econlib.org/library/LFBooks/Burke/brkSWv4c4.html.

Caraway, Brett. 2011. "Audience Labor in the New Media Environment: A Marxian Revisiting of the Audience Commodity." *Media, Culture & Society* 33 (5): 693-708.

Card, Stuart K., Thomas P. Moran, and Allen Newell. 1990. *The Psychology of Human-Computer Interaction.* Hillsdale: Lawrence Erlbaum Associates.

Carr, Nicholas. 2016. "Digital Sharecropping." In *Utopia Is Creepy*, by Nicholas Carr, 30-31. New York: W. W. Norton and Company.

Carrascal, Juan Pablo, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo de Oliveira. 2013. "Your browsing behavior for a big mac: economics of personal information online." *Proceedings of the 22nd international conference on World Wide Web.* Geneva: International World Wide Web Conferences Steering Committee. 189-200.

Castells, Manuel. 2012. *Networks of Outrage and Hope: Social Movements in the Internet Age.* Cambridge: Polity Press.

Cavoukian, Ann. 2009. *Privacy by Design.* Toronto: Information and Privacy Commissioner of Ontario.

Cavoukian, Ann, and Mark Dixon. 2013. *Privacy and Security by Design: An Enterprise Architecture Approach.* Toronto: Information and Privacy Commissioner.

CBC News. 2013. *Privacy commissioner to investigate Bell's data collecting.* October 22. Accessed September 11, 2015. http://www.cbc.ca/news/canada/montreal/privacy-commissioner-to-investigate-bell-s-data-collecting-1.2158593.

Celis Bueno, Claudio. 2017. *The Attention Economy: Labour, Time and Power in Cognitive Capitalism.* London: Rowman & Littlefield.

Chang, Shu-Nu. 2007. "Externalising students' mental models through concept maps." *Journal of Biological Education* 41 (3): 107-112.

Chen, Eric Y., Yutong Pei, Shuo Chen, Yuan Tian, Robert Kotcher, and Patrick Tague. 2014. "OAuth Demystified for Mobile Application Developers." *CCS '14 Proceedings of the*

2014 ACM SIGSAC Conference on Computer and Communications Security. Scottsdale: ACM. 892-903.

Cheney-Lippold, John. 2011. "A NewAlgorithmic Identity: Soft Biopolitics and the Modulation of Control." *Theory, Culture & Society* 28 (6): 164-181.

Cherrueau, Ronan-Alexandre, Rémi Douence, Jean-Claude Royer, Mario Südhol, Anderson Santana de Oliveira, Yves Roudier, and Matteo Dell'Amico. 2014. "Reference monitors for security and interoperability in OAuth 2.0." In *Data Privacy Management and Autonomous Spontaneous Security*, edited by Joaquin Garcia-Alfaro, Georgios Lioudakis, Nora Cuppens-Boulahia, Simon Foley and William M. Fitzgerald, 235-249. Berlin: Springer.

Chiasson, Sonia, and Robert Biddle. 2007. "Issues in User Authentication." *Computer/Human Interaction.* San Jose. 1-4.

Clark, David. 2012. "Control Point Analysis." *TPRC, 40th Research Conference on Communication, Information and Internet Policy.* Arlington. 1-25.

Cleaver, Harry. 1979. *Reading Capital Politically.* Austin: University of Texas Press.

Cohen, Barry H., and Brooke R. Lea. 2004. *Essential Statistics for the Social and Behavioral Sciences.* New Jersey: John Wilwy & Sons.

comScore. 2016. *comScore Releases February 2016 U.S. Desktop Search Engine Rankings.* March 16. Accessed February 10, 2017. http://www.comscore.com/Insights/Rankings/comScore-Releases-February-2016-US-Desktop-Search-Engine-Rankings.

Cook, Thomas D., and T. Donald Campbell. 1979. *Quasi-Experimentation: Design & Analysis Issues for Field Testing.* Chicago: Rand McNally College Publishing Company.

Coopamootoo, Kovila P.L., and Thomas Groß. 2014. "Mental Models for Usable Privacy: A Position Paper." *Human aspects of information security, privacy, and trust : second International Conference.* Heraklion.

Corbin, Juliet, and Anselm Strauss. 1990. "Grounded Theory Research: Procedures, Canons and Evaluative Criteria." *Zeitschrift für Soziologie* 19 (6): 418-427.

Coventry, Lynne. 2005. "Usable Biometrics." In *Usable Security: Designing Secure Systems that People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, 175-197. Sebastopol: O'Reilly.

Craik, Kenneth. 2010. *The Nature of Explanation.* Cambridge: Cambridge University Press.

Cranor, Lorrie Faith. 2005. "Privacy and Privacy Preferences." In *Security and Usability: Designing Secure Systems that People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, 447-471. Sebastapol: O'Reilly.

Cranor, Lorrie Faith, Praveen Guduru, and Manjula Arjula. 2006. "User Interfaces for Privacy Agents." *ACM Transactions on Computer-Human Interaction* 13 (2): 135–178.

CRTC. 2016. *Politique réglementaire de télécom CRTC 2016-496.* Governnment, Ottawa: Conseil de la radiodiffusion et des télécommunications canadiennes.

CrtlShift. 2016. *A New Paradigm for Personal Data: Five Shifts to Drive Trust and Growth.* London: CrtlShift. www.facebook.com/anewdataparadigm.

CrunchBase. 2015. *Facebook.* Accessed September 2, 2015. https://www.crunchbase.com/organization/facebook#x.

Crunchbase. 2015. *Facebook Connect.* Accessed September 2, 2015. https://www.crunchbase.com/product/facebook-connect.

Culnan, Mary J. 2000. "Protecting privacy online: Is self-regulation working?" *Journal of Public Policy & Marketing* 19 (1): 20-26.

D'Angelo, Paul, and Jim A. Kuypers. 2010. "Introduction: Doing News Framing Analysis." In *Doing News Framing Analysis: Empirical and Theoretical Perspectives*, edited by Paul D'Angelo and Jim A. Kuypers, 1-13. New York: Routledge.

Davenport, Thomas H., and John C. Beck. 2002. *The Attention Economy: Understanding the New Currency of Business.* Brighton: Harvard Business Press.

Davis, Murray S. 1997. "Georg Simmel and Erving Goffman: Legitimators of the Sociological Investigation of Human Experience." *Qualitative Sociology* 20 (3): 380.

Day, Ronald E. 2001. *The Modern Invention of Information: Discourse, History, and Power.* Carbondale and Edwardsville: Southern Illinois University Press.

Denham, Elizabeth. 2009. *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. aux termes de la Loi sur la protection des renseignements personnels et les docu.* Rapport de conclusions, Commissariat à la protection de la vie privée du Canada, Ottawa: Commissariat à la protection de la vie privée du Canada.

dlvr.it. 2009. *dlvr.it Privacy Policy.* November 16. Accessed April 5, 2017. https://dlvrit.com/privacy-policy.

Dourish, Paul. 2001. *Where The Action Is: The Foundations of Embodied Interaction.* Cambridge: MIT Press.

Dourish, Paul, Rebecca E. Grinter, Jessica Delgado de la Flor, and Melissa Joseph. 2004. "Security in the wild: user strategies for managing security as an everyday, practical problem." *Personal Ubiquitous Computing* (8): 391-401.

Dretske, Fred. 2006. "Perception without Awareness." In *Perceptual Experience*, edited by Tamar Szabo Gendler and John Hawthorne, 147-180. Oxford: Oxford.

Dubé, Adam K., and Rhonda N. McEwen. 2015. "Do gestures matter? The implications of using touchscreen devices in mathematics instruction." *Learning and Instruction* 40: 89-98.

2010. *The Social Network.* Directed by David Fincher. Performed by Jesse Eisenberg, Andrew Garfield and Justin Timberlake.

Ellis, Rod, and Fangyuan Yuan. 2004. "The Effects of Planning On Fluency, Complexity, and Accuracy In Second Language Narrative Writing." *Studies in Second Language Acquisition* (Cambridge University Press) 26 (1): 59-84.

Englehardt, Yuri von. 2002. *The language of graphics.* Dissertation, Uniiversity of Amesterdam.

Facebook. 2015. *About.* Accessed September 2, 2015. https://www.facebook.com/facebook/info?tab=milestone.

—. 2015. *Audience Optimization.* Facebook. Accessed January 23, 2017. https://www.facebook.com/facebookmedia/get-started/audience-optimization.

Facebook Business. 2016. *Announcing New Partners for Advert Viewability Verification.* April 19. Accessed February 8, 2017. https://www.facebook.com/business/news/new-ad-viewability-partners.

Facebook. 2016. *Data Policy.* September 29. Accessed January 9, 2017. https://www.facebook.com/privacy/explanation.

—. 2017. *Facebook Platform Policy.* Accessed February 1, 2017. https://developers.facebook.com/policy.

Facebook for Developers. n.d. *Permissions Reference - Facebook Login.* Accessed February 8, 2017. https://developers.facebook.com/docs/facebook-login/permissions.

Feenberg, Andrew. 1999. *Questioning Technology.* London: Routledge.

Foster, Pauline, Alan Tonkyn, and Gillian Wigglesworth. 2000. "Measuring Spoken Language: A Unit for All Reasons." *Applied Linguistics* (Oxford University Press) 21 (3): 354±375.

Fuchs, Christian. 2012. "Dallas Smythe today - the audience commodity, the digital labour debate, Marxist Political Economy and Critical Theory. Prolegomena to a digital labour theory of value." *TripleC* 10 (2): 692-740.

—. 2014. *Social Media: A Critical Introduction.* London: Sage.

Fuchs, Christian. 2012. "The Political Economy of Privacy on Facebook." *Television & New Media* 13 (2): 139-159.

Garg, V., and L. J. Camp. 2014. "Risk Characteristics, Mental Models, and Perception of Security Risks." *2014 ASE BigData/SocialInformatics/PASSAT/BioMedCom Conference.* Cambridge: Academy of Science and Engineering. 1-10.

Gentner, Donald R., and Jonathan Grudin. 1996. "Design Models for Computer-Human Interfaces." *Computer* 29 (6): 28-35.

Gepshtein, Sergei. 2010. "Two psychologies of perception and the prospect of their synthesis." *Philosophical Psychology* 23 (2): 217-281.

Gerber, Paul, Melanie Volkamer, and Karen Renaud. 2015. "Usability versus Privacy instead of Usable Privacy: Google's balancing act between usability and privacy]." *SIGCAS Computers & Society* 45 (1): 16-21.

Gerlinger, Jan. 2013. *Stack Overflow: Does Twitter support OAuth 2.0?* May 27. Accessed February 13, 2017. http://stackoverflow.com/questions/16769777/does-twitter-support-oauth-2-0.

Gibbons, Kevin, John O'Raw, and Kevin Curran. 2014. "Security Evaluation of the OAuth 2.0 Framework." *Information Management and Computer Security* 22 (3).

Giddens, Anthony. 1984. *The Constitution of Society.* Cambridge: Polity Press.

Gillespie, Tarleton. 2010. "The Politics of 'Platforms'." *New Media & Society* 12 (3): 347–364.

Glynn, Shawn. 1997. "Drawing Mental Models." *The Science Teacher*, January: 30-32.

Godin, Dan. 2015. *Gigabytes of user data from hack of Patreon donations site dumped online.* October 1. Accessed October 30, 2015. http://arstechnica.com/security/2015/10/gigabytes-of-user-data-from-hack-of-patreon-donations-site-dumped-online/.

Goffman, Erving. 1974. *Frame Analysis: An Essay on the Organization of Experience.* Cambridge: Harvard University Press.

—. 1971. *The presentation of self in everyday life.* Harmondsworth: Penguin.

Goldhaber, Michael H. 1997. "The Attention Economy and the Net." *First Monday - Peer-Reviewed Journal on the Internet* 2 (4). Accessed March 10, 2017. http://firstmonday.org/ojs/index.php/fm/article/view/519/440.

Gomez-Ortigoza, Anaid. 2016. *New Video Metrics: Understand the Audience and Engagement of Your Facebook Videos.* Facebook. August 10. Accessed January 23, 2017. https://media.fb.com/2016/08/10/new-video-metrics-understand-the-audience-and-engagement-of-your-facebook-videos/.

Google. 2004. *Google Gets the Message, Launches Gmail.* April 1. Accessed October 2, 2017. http://googlepress.blogspot.ca/2004/04/google-gets-message-launches-gmail.html.

Google. n.d. "Google Sign-in for Doodle." Case study. Accessed December 10, 2016. https://developers.google.com/identity/casestudies/doodle-signin-casestudy.pdf.

Google. n.d. "Google Sign-In for Luxe." Case study. Accessed April 3, 2017. https://developers.google.com/identity/casestudies/luxe-signin-casestudy.pdf.

Google. n.d. "Google Sign-in for Moovit." Case study. Accessed December 10, 2016. https://developers.google.com/identity/casestudies/moovit-signin-casestudy.pdf.

—. 2016. *Privacy Policy.* August 29. Accessed September 13, 2016. https://www.google.com/policies/privacy/.

—. 2017. *Verify your Google Account.* Accessed January 26, 2017. https://support.google.com/accounts/answer/63950?hl=en&ref_topic=7188671.

Green, Thomas R.G. 1990. "Limited Theories as a Framework for Human-Computer Interaction." In *Mental Models and Human-Computer Interaction 1*, edited by D. Ackermann and M.J. Tauber, 5-39. North-Holland: Elsevier Science Publishers.

Grossklags, Jens, and Nathan Good. 2007. "Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers." *Financial Cryptography and Data Security.* 341-355.

Grudin, Jonathan. 2012. "A Moving Target: The Evolution of Human-Computer Interaction." In *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications*, edited by Julie A. Jacko, xxvii-lxi. CRC Press: Boca Raton.

Hammer-Lahav, Eran. 2010. *hueniverse: Introducing OAuth 2.0.* May 10. Accessed February 13, 2017. https://hueniverse.com/2010/05/15/introducing-oauth-2-0/.

—. 2007. *OAuth: Introduction.* September 5. Accessed February 13, 2017. https://oauth.net/about/introduction/.

Hans, G.S. 2013. "Privacy Policies, Terms of Service, and FTC Enforcement: Broadening Unfairness Regulation for a New Era." *Michigan Telecommunications and Technology Law Review* 19 (2): 163-197.

Harvey, David. 2010. *A Companion to Marx's Capital.* London: Verso.

—. 1989. *The Condition of Postmodernity.* Cambridge: Blacwell Publisher.

Hashemi, Yasamine. 2009. "Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability." *University Journal of Science Technology Law* 15 (1): 140-161.

Hassenzahl, Marc. 2008. "User experience (UX): towards an experiential perspective on product quality." *Proceedings of the 20th International Conference of the Association Francophone d'Interaction Homme-Machine.* Metz: ACM. 11-15.

Heyman, Rob, Ralf De Wolf, and Jo Pierson. 2014. "Evaluating social media privacy settings for personal and advertising purposes." *Digital Policy, Regulation and Governance* 16 (4): 18-32.

Hockey, G. Robert J. 1990. "Styles, Skills and Strategies: Cognitive Variability and its Implications for the Role of Mental Models in HCI." In *Mental Models and Human-Computer Interaction 1*, 112-129. North-Holland: Elsevier Science Publishers.

Huizinga, Johan. 1970. *Homo Ludens: A Study of the Play Element in Culture.* Translated by George Steiner. London: Maurice Temple Smith.

Hunter, Brent. 2015. *Farewell to Facebook webOS Synergy/App.* April 2015. Accessed April 30, 2017. https://pivotce.com/2015/04/03/farewell-to-facebook-webos-synergyapp/.

Internet Engineering Task Force. 2010. *The OAuth 1.0 Protocol.* April. Accessed February 13, 2017. https://tools.ietf.org/html/rfc5849.

Jameson, Fredric. 1976. "On Goffman's Frame Analysis." *Theory and Society* 3 (1): 119-133.

Jensen, Carlos, and Colin Potts. 2004. "Privacy Policies as Decision-Making Tools: An Evaluation of Online Privacy Notices." *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* Vienna. 471-478.

Johnson, Maritza, Serge Egelman, and Steven M. Bellovin. 2012. "Facebook and Privacy: It's Complicated." *SOUPS '12 Proceedings of the Eighth Symposium on Usable Privacy and Security* . Washington, D.C.

Johnson-Laird, P. N. 2013. "Mental models and cognitive change." *Journal of Cognitive Psychology* 25 (2): 131-138.

Johnson-Laird, Philip N. 2010. "Mental models and human reasoning." *Proceedings of the National Academy of Sciences of the United States of America* 107 (43): 18243-18250.

—. 1983. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness.* Cambridge: Harvard University Press.

—. 1983. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness.* Cambridge: University Press of Cambridge.

Johnston, Anna, and Stephen Wilson. 2012. "Privacy Compliance Risks for Facebook." *IEEE Technology and Society Magazine*, June 6: 59-64.

Johnston, Hank. 1995. *A Methodology for Frame Analysis: From Discourse to Cognitive Schemata.* Vol. 4, in *Social Movements and Culture: Social Movements, Protest, and Contention*, edited by Hank Johnston and Bert Klandermans, 217-246. Minneapolis: University of Minnesota Press.

Kahn, David. 1996. *The Codebreakers.* New York: Scribner.

Keenan, Andrew. 2016. "Literature review." *Gameplay In An Unfamiliar Environment: Novice and Expert Adult Players Encountering Portal For The First Time.* University of Toronto.

Kemmerer, David. 2006. "The semantics of space: Integrating linguistic typology and cognitive neuroscience." *Neuropsychologia* 44 (9): 1607–1621.

Kerskovits, Annette. 1986. *Language and Spatial Cognition: An interdisciplinary study of the prepositions in English.* Cambridge: Cambridge University Press.

Kline, Douglas M., Ling He, and Ulku Yalaciecegi. 2011. "User Perceptions of Security Technologies." *International Journal of Information Security and Privacy* 5 (2): 1-12.

Kuehn, Andreas. 2013. "Cookies versus clams: clashing tracking technologies and online privacy." *Info* 15 (6): 19-31.

Kuhn, Markus G., and Ross J. Anderson. 1998. "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations." In *Information Hiding*, edited by David Aucsmith, 124-142. Berlin: Springer-Verlag.

Kushner, Scott. 2016. "Read Only: The Persistence of Lurking in Web 2.0." *First Monday: Peer Reviewed Journal on the Internet* 21 (6). Accessed July 7, 2016. doi:http://dx.doi.org/10.5210/fm.v21i6.6789.

Kuypers, Jim A. 2009. "Framing Analysis." In *Rhetorical Criticism*, edited by Jim A. Kuypers, 181-203. Lanham: Lexington Books.

Lafferman, Matthew. 2012. "Do Facebook and Twitter Make You a Public Figure: How to Apply the Gertz Public Figure Doctrine to Social Media." *Santa Clara Computer and High Technology Law Journal* 29: 199-247.

Lederer, Scott, Jason I. Hong, Anind K. Dey, and James A. Landay. 2005. "Five Pitfalls in the Design for Privacy." In *Security and Usability: Designing Secure Systems that People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, 421-445. Sebastapol: O'Reilly.

Lee, Micky. 2014. "From Google to Guge: The Political Economy of a Search Engine." In *The Audience Commodity in the Digital Age*, edited by Lee McGuigan and Vincent Manzerolle, 175-191. New York: Peter Lang Publishing.

Lee, Micky. 2011. "Google Ads and the Blindspot Debate." *Media, Culture & Society* 33 (3): 433-447.

Legal Information Institute. 2002. *44 U.S. Code § 3542 - Definitions.* December 17. Accessed April 10, 2015. https://www.law.cornell.edu/uscode/text/44/3542.

Lievrouw, Leah. 2002. "Determination and Contingency in New Media Development: Diffusion of Innovations and Social Shaping of Technology Perspectives." In *The Handbook of New Media: Social Shaping and Consequences of ICTs*, edited by Leah Lievrouw and Sonia Livingstone, 183-199. London: Sage.

Light, Ben. 2014. *Disconnecting with Social Networking Sites.* New York: Palgrave MacMillan.

Lindsay, David. 2005. "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law." *Melbourne University Law Review* 29: 131-178.

Lockhart, Harold. 2005. *Demystifying SAML.* October 11. Accessed February 13, 2017. http://www.oracle.com/technetwork/articles/entarch/saml-084342.html.

Mackenzie, I. Scott. 2013. *Human-Computer Interaction: An Empirical Research Perspective.* Waltham, Massachusetts: Elsevier.

Malvern, David, and Brian Richards. 2002. "Investigating accommodation in language proficiency interviews using a new measure of lexical diversity." *Language Testing* 19 (1): 85-104.

Manzerolle, Vincent. 2014. "Technologies of Immediacy / Economies of Attention: Notes on the Commercial Development of Mobile Media and Wireless Connectivity." In *The Audience Commodity in the Digital Age*, edited by Lee McGuigan and Vincent Manzerolle, 207-226. New York: Peter Lang Publishing.

Marache-Francisco, Cathie, and Éric Brangier. 2015. "The Gamification Experience: UXD with a Gamification Background." In *Gamification: Concepts, Methodologies, Tools, and Applications*, 1-20. Information Science Reference.

Marx, Karl. 1990. *Capital Volume One: A Critique of Political Economy.* Translated by Ben Fowkes. Vol. One. London: Penguin Books.

—. 1992. *Capital Volume Two: A Critique of Political Economy.* Translated by David Ferbach. London: Penguin Books.

Marx, Karl. 1978. "The German Ideology: Part I." In *The Marx-Engels Reader*, by Karl Marx and Friedrich Engels, edited by Robert C. Tucker, translated by Martin Nicolaus, 146-200. New York: W.W Norton & Company Inc.

Maybee, Julie E. 2016. "Hegel's Dialectics." *The Stanford Encyclopedia of Philosophy.* Summer Edition. Accessed July 13, 2016. http://plato.stanford.edu/archives/sum2016/entries/hegel-dialectics.

McCracken, Harry. 2014. "How Gmail Happened: The Inside Story of Its Launch 10 Years Ago." *Time*, Arch 31. Accessed October 2, 2017. http://time.com/43263/gmail-10th-anniversary/.

McEwen, Rhonda, and Kathleen Scheaffer. 2013. "Virtual Mourning and Memory Construction on Facebook: Here are the Terms of Use." *Bulletin of Science, Technology & Society* 33 (3-4): 64-75.

McLuhan, Marshall. 1994. *Understanding Media: The Extension of Man.* First MIT Press edition, 1994. Cambridge: The MIT Press.

McNeal, Gregory S. 2014. *Controversy Over Facebook Emotional Manipulation Study Grows As Timeline Becomes More Clear.* June 30. Accessed February 1, 2017. https://www.forbes.com/sites/gregorymcneal/2014/06/30/controversy-over-facebook-emotional-manipulation-study-grows-as-timeline-becomes-more-clear/#1f2187b09caa.

McNeil, Sara, and Larry Butts. 2003. "Mental Models: Using Visual Concept Maps To Understand the Multimedia Learning Process." *Society for Information Technology & Teacher Education International Conference.* Chesapeake: Association for the Advancement of Computing in Education. 1496-1502.

Meehan, Eileen. 1993. "Commodity Audience, Actual Audience: The Blindspot Debate." In *Illuminating the Blindspots: Essays Honoring Dallas W. Smythe*, edited by Janet Wasko, Vincent Mosco and Manjunath Pendakur, 378-397. Norwood, New Jersey: Ablex Publishing Corporation.

Mihajlov, Martin, Saso Josimovski, and Borka Jerman-Blazič. 2011. "A Conceptual Framework for Evaluating Usable Security in Authentication Mechanisms – Usability Perspectives." *2011 5th International Conference on Network and System Security.* 332-336.

Milazzo, Michael J. 2014. "Facebook, Privacy, and Reasonable Notice: The Public Policy Problems with Facebook's Current Sign-Up Process and How to Remedy the Legal Issues." *Cornell Journal of Law and Public Policy* 99 (5): 661-688.

Miller, Hugh. 1995. "The Presentation of Self in Electronic Life: Goffman on the Internet." *Embodied Knowledge and Virtual Space Conference Goldsmiths' College, University of London.* London: University of London. 1-8. Accessed June 29, 2015. http://www.dourish.com/classes/ics234cw04/miller2.pdf.

Milne, George R., and Mary J. Culnan. 2004. "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices." *Journal of Interactive Marketing* 18 (3): 15-29.

Monrose, Fabian, and Michael K. Reiter. 2005. "Graphical Passwords." In *Security and Usability: Designing Secure Systems that People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, 157-174. Sebastopol: O'Reilly.

Moulier Boutang, Yann. 2008. *Le Capitalisme cognitif: La Nouvelle grande transformation.* Paris: Éditions Amsterdam.

Munshi, Soumyanetra. 2010. "Enfranchisement from a political perspective." *Constitutional Political Economy* 22 (1): 21–57.

Munzer, Stephen R. 2005. "Property." In *The Shorter Routledge Encyclopedia of Philosophy*, edited by Edward Craig, 858-861. London: Routledge.

Napoli, Philip M. 2014. "The Institutionally Effective Audience in Flux: Social Media and the Reassessment of the Audience Commodity." In *The Audience Commodity in the Digital Age*, edited by Lee McGuigan and Vincent Manzerolle, 115-133. New York: Peter Lang Publishing.

Newman, Mark E. J. 2010. "Technological Networks." In *Networks: An Introduction*, by Mark E. J. Newman, 17-35. Oxford: Oxford University Press.

Nissenbaum, Helen. 1997. "Toward an Approach to Privacy in Public: Challenges of Information Technology." *Ethics & Behavior* 7 (3): 207-219.

Noam, Eli. 1997. "Privacy and Self-Regulation: Markets for Electronic Privacy." In *Privacy and Self-Regulation in the Information Age*. Washington, DC: National Telecommunications and Information Administration. Accessed June 9, 2017. https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy.

Norman, Don. 1983. "Some Observations on Mental Models." In *Mental Models*, edited by Dedre Gentner and Albert L Stevens, 7-14. Hillsdale, New Jersey: Lawrence Erlbaum Associates, Inc.

—. 2013. *The Design of Everyday Things: Revised and Expanded Edition.* New York: Basic Books.

Norman, Donald A. 1986. "Cognitive Engineering." In *User Centered System Design*, edited by Donald A. Norman and Stephen W. Draper, 31-61. Hillsdale: Lawrence Erlbaum Associates, Publishers.

Norman, Donald A. 1983. "Design rules based on analyses of human error." *Communications of the ACM* 26 (4): 254-258.

O'Connor, Debra L., Tristan E. Johnson, and Mohammed K. Khalil. 2008. "Measuring Team Cognition: Concept Mapping Elicitation as a Means of Constructing Team Shared Mental Models in an Applied Setting." *Performance Improvement Quarterly* 21 (3): 113-134.

O'Dell, Jolie. 2011. *Twitter to Devs: Don't Make Twitter Clients... Or Else.* March 11. Accessed April 30, 2017. http://mashable.com/2011/03/11/twitter-api-clients/#HK3Yh.SsnEqs.

OneLogin. 2015. *OneLogin Developers: Best Practices & FAQs.* Accessed February 13, 2017. https://developers.onelogin.com/saml/best-practices-and-faqs.

OpenID. 2017. *OpenID Connect FAQ and Q&As.* Accessed February 12, 2017. http://openid.net/connect/faq/.

Otter, M., and H. Johnson. 2000. "Lost in hyperspace: metrics and mental models." *Interacting with Computers* 13 (1): 1-40.

Parecki, Aaron. 2012. *OAuth 2 Simplified.* July 29. Accessed February 13, 2017. https://aaronparecki.com/2012/07/29/7/oauth2-simplified.

—. 2016. *OAuth.com: Background.* August 30. Accessed February 13, 2017. https://www.oauth.com/oauth2-servers/background/.

Parker, Donn B. 1998. *Fighting Computer Crime: A New Framework for Protecting Information.* New York: Wiley Computer Publishing.

Pasquale, Frank. 2015. *The Black Box Society.* Cambridge: Harvard University Press.

Payne, Bryan D., and W. Ketih Edwards. 2008. "A Brief Introduction to Usable Security." *IEEE Internet Computing* 13-21.

Pence, Janet T., John W. Cotton, Benton J. Underwood, and Carl P. Duncan. 1992. *Elementary Statistics: Revised Fifth Edition.* New Jersey: Prentice Hall.

Pierre, Fritz, Mohamed Ayad, and Hédi Jemai. 1985. *Planification familiale, fécondité et santé familiale en Haïti, 1983 : rapport sur les résultats de l'enquête haïtienne sur la prévalence de la contraception.* Columbia, Md: Westinghouse Public Applied Systems.

Pinch, Trevor, and Wiebe Bijker. 1987. "The Social Construction of Facts and Artifacts: Or, How the Sociology of Science and the Sociology of Technology Might Benefit Each Other." In *The Social Construction of Technological Systems: : New directions in the sociology and history of technology*, edited by Wiebe Bijker, Thomas Hughes, Trevor Pinch and Deboorah G. Douglas, 17-50. Cambridge: MIT Press.

Pinch, Trevor, and Wiebe E. Bijker. 1987. "The Social Construction of Facts and Artifacts: Or, How the Sociology of Science and the Sociology of Technology Might Benefit Each Other." In *The Social Construction of Technological Systems*, edited by Wiebe E. Bijker, Thomas P. Hughes and Trevor Pinch, 17-50. Cambridge, Massachusetts: MIT Press.

Post, Robert C. 1986. "The Social Foundations of Defamation Law: Reputation and the Constitution." *California Law Review* 74 (3): 691-742.

Postman, Neil. 1986. *Amusing Ourselves to Death: Public Discourse in the Ageof Show Business.* London: William Heinemann.

Pridmore, Jason, and Daniel Trottier. 2014. "Extending the Audience: Social Media Marketing, Technologies and the Construction of Markets." In *The Audience Commodity in the Digital Age*, edited by Lee McGuigan and Vincent Manzerolle, 135-155. New York: Peter Lang Publishing.

Prosser, Jon, and Andrew Loxley. 2008. *Introducing Visual Methods.* Southampton: National Centre for Research Methods.

Rapp, Amon. 2015. "A Qualitative Investigation of Gamification: Motivational Factors in Online Gamified Services and Applications." In *Gamification: Concepts, Methodologies, Tools, and Applications*, 32-48. Information Science Reference.

Rayward, Boyd W. 1983. "Library and Information Sciences: Disciplinary Differentiation, Competition, and Convergence." In *The Study of Information: : Interdisciplinary Messages*, edited by Fritz Machlup and Una Mansfield, 343-369. New York: John Wiley & Sons.

Reason, James. 2000. "Human error: models and management." *BMJ : British Medical Journal* 320 (7237): 768–770.

Reimer, Tim, Phil Abraham, and Qing Tan. 2013. "Federated Identity Access Broker Pattern for Cloud Computing." *2013 16th International Conference on Network-Based Information Systems.* IEEE. 134-140.

Reitman, Rainey. 2012. *What Actually Changed in Google's Privacy Policy.* February 1. Accessed October 2, 2017. https://www.eff.org/deeplinks/2012/02/what-actually-changed-google's-privacy-policy.

Renaud, Karen. 2003. "Quantifying the Quality of Web Authentication Mechanisms. A Usability Perspective." *Journal of Web Engineering* 3 (2): 95-123.

Rigi, Jakob, and Robert Prey. 2015. "Value, Rent, and the Political Economy of Social Media." *The Information Society* 31 (5): 392–406.

Robison, Richard. 2008. "Google: A Chronology of Innovations, Acquisitions, and Growth." *Journal of Library Administration* 46 (3-4): 5-29.

Rosen, David. 2012. *How Telecoms Sell Your Private Info to the Highest Bidder.* November 8. Accessed September 11, 2015. http://www.alternet.org/civil-liberties/how-telecoms-sell-your-private-info-highest-bidder.

Rubinstein, Ira S., and Nathaniel Good. 2012. "Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents." *Berkerley Technology Law Journal* 28: 1333-1414.

Saltzer, Jerome H., and Michael D. Schroeder. 1975. "The Protection of Information in Computer Systems." *Proceedings of the IEEE.* Cambridge: ACM. 1278-1308.

SANS Institute Reading Room. 2017. *An Introduction to TEMPEST.* Bethesda: SANS Institute. https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981.

Sasse, Martina Angela. 1997. *Eliciting and Describing Users' Models of Computer Systems.* Dissertation, School of Computer Science, University of Birmingham, Birmingham: University of Birmingham.

Sasse, Martina Angela, and Ivan Flechais. 2005. "Usable Security: Why Do We Need It? How Do Get It?" In *Security and Usability: Designing Secure Systems that People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, 13-30. Sebastopol: O'Reilly.

Sauro, Jeff, and James R. Lewis. 2012. *Quantifying the User Experience: Practical Statistics for User Research.* 1st Edition. Amsterdam: Morgan Kaufmann.

Savolainen, Reijo. 2008. *Everyday Information Practices: A Social Phenomenon.* Lanham: The Scarecrow Press.

Schonfeld, Erick. 2011. *The HP TouchPad Will Come With Its Own Facebook Tablet App (Leaked Pics).* June 27. Accessed April 30, 2017. https://techcrunch.com/2011/06/27/facebook-tablet-app-hp-touchpad/.

Schultz, Eugene E., Robert W. Proctor, Mei-Ching Lien, and Gavriel Salvendy. 2001. "Usability and Security An Appraisal of Usability Issues in Information Security Methods." *Information Security Methods Computers & Security* 20 (7): 620-634.

Schumpeter, Joseph A. 2013. *Capitalism, Socialism and Democracy.* London: Routledge.

Shy, Oz. 2008. "Demand and Cost." In *How to Price: A Guide to Pricing Techniques and Yield Management*, by Oz Shy, 19-58. Cambridge: Cambridge University Press.

Siegel, Max. 1979. "Privacy, ethics, and confidentiality." *Professional Psychology* 10 (2): 249-258.

Simmel, Georg. 2002. "The Metropolis and Mental Life." In *The Blackwell City Reader*, edited by Gary Bridge and Sophie Watson, 11-19. Oxford and Malden: Wiley-Blackwell.

—. 1978. *The Philosphy of Money.* Edited by David Frisby. Translated by Tom Bottomore, David Frisby and Kaethe Mengelberg. London: Routledge.

Simon, Herbert A., Karl W. Deutsch, Martin Shubik, and Emilio Q. Daddario. 1971. "Designing Organizations for an Information-rich world." In *Computers, communications, and the public interest*, edited by Martin Greenberger, 37-72. Baltimore: Johns Hopkins Press.

Smith, P.F. 1994. "Enfranchisement of Flats and Right to an Individual New Long Lease: A Critical Evaluation." *Property Management* 12 (2): 34-49.

Smythe, Dallas W. 1977. "Communications: Blindspot of Western Capitalism." *Canadian Journal of Political and Social Theory/Revue canadienne de théorie politique et sociale* 1 (3): 1-27.

Staiano, Jacopo, Nuria Olive, Bruno Lepri, Rodrigo de Oliveira, Michele Caraviello, and Nicu Sebe. 2014. "Money Walks: A Human-Centric Study on the Economics of Personal Mobile Data." *ACM International Joint Conference on Pervasive and Ubiquitous Computing.* Seattle. 583-594.

Statt, Nick. 2016. *Facebook is giving up on BlackBerry.* March 21. Accessed April 30, 2017. http://www.theverge.com/2016/3/21/11279934/facebook-drops-blackberry-support-whats-app.

Stein, Laura. 2013. "Policy and Participation on Social Media: The Cases of YouTube, Facebook, and Wikipedia." *Communication , Culture & Critique* 6: 353-371.

St-Louis, Hervé. 2011. *Iranian Political Unrest on Twitter.* Master's Thesis, Centre for Military and Stretegic Studies, University of Calgary, Calgary: University of Calgary.

Suchman, Lucy. 2007. *Human-Machine Reconfigurations: Plans and Situated Actions.* 2nd Edition. Cambridge: Cambridge University Press.

Suits, Bernard. 1978. *The Grasshopper: Games. Life and Utopia.* Toronto: University of Toronto Press.

Sun, San-Tsai, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. 2013. "Investigating Users' Perspectives of Web Single Sign-On: Conceptual Gaps and Acceptance Model." *ACM Transactions on Internet Technology* 13 (1): 2-35.

Sutton-Smith, Brian. 1997. *The Ambiguity of Play.* Cambridge, Massachusetts: Harvard University Press.

Terranova, Tiziana. 2004. *Network Culture: Politics for the Information Age.* New York: Pluto Press.

Tullis, Thomas, and William Albert. 2013. *Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics.* 2nd Edition. Amsterdam: Morgan Kaufmann.

Twitter. 2017. *Twitter Developer Documentation: Authorizing a request.* Accessed February 13, 2017. https://dev.twitter.com/oauth/overview/authorizing-requests.

—. 2016. *Twitter Privacy Policy.* September 30. Accessed May 1, 2017. https://twitter.com/privacy?lang=en.

Umoquit, Muriah J., Peggy Tso, Helen ED Burchett, and Mark J. Dobrow. 2011. "A multidisciplinary systematic review of the use of diagrams as a means of collecting data from research subjects: application, benefits and recommendations." *BMC Medical Research Methodology* 11 (11): 1-10.

Umoquit, Muriah, Peggy Tso, Tünde Varga-Atkins, Mark O'Brien, and Johannes Wheeldon. 2013. "Diagrammatic Elicitation: Defining the Use of Diagrams in Data Collection." *The Qualitative Report* 18 (30): 7-29.

Van Fleet, Connie, and Danny P. Wallace. 2002. "The I-word: Semantics and Substance in Library and Information Studies Education." *Reference & User Services Quarterly* 42 (2): 105-109.

Warren, Tom. 2014. *Windows' best Twitter client is about to die.* March 5. Accessed April 30, 2017. http://www.theverge.com/2014/3/5/5473110/metrotwit-for-windows-end-of-support.

Waters, Samuel R. 2012. *Web--based Single Sign-On: An examination of security and usability.* Thesis, B. Thomas Golisano College of Computing and Information Sciences, Rochester Institute of Technology, Ann Arbor: ProQuest.

Weir, Catherine S., Gary Douglas, Tim Richardson, and Mervyn Jack. 2010. "Usable security: User preferences for authentication methods in eBanking and the effects of experience." *Interacting with Computers* (22): 153-164.

Wenger, Étienne. 1998. *Communities of practice: learning, meaning, and identity.* Cambridge: Cambridge University Press.

Werbin, Kenneth C. 2012. "Auto-biography: On the Immanent Commodification of Personal Information." *International Review of Information Ethics* 17 (17): 46-53.

Wheeldon, Johannes, and Jacqueline Faubert. 2009. "Framing Experience: Concept Maps, Mind Maps, and Data Collection in Qualitative Research." *International Journal of Qualitative Methods* 8 (3): 68-83.

Whitten, Alma. 2012. *Updating our privacy policies and terms of service.* January 24. Accessed October 2, 2017. https://googleblog.blogspot.ca/2012/01/updating-our-privacy-policies-and-terms.html.

Whitten, Alma, and J.D. Tygar. 2005. "Why Johnny Can't Encrypt: A Usability Wvaluation of PGP 5.0." In *Security and Usability*, edited by Lorrie Faith Cranor and Simson Garfinkel, 669-692. Sebastopol: O'Reilly.

Williams, Christopher. 2015. *Google charged with monopoly abuse.* April 15. Accessed February 10, 2017. http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/11537546/Google-charged-with-monopoly-abuse.html.

Williams, Robin, and David Edge. 1996. "The Social Shaping of Technology." *Research Policy* 25: 865-899.

Wilson, Robert E., Samuel D. Gosling, and Lindsay T. Graham. 2012. "A Review of Facebook Research in the Social Sciences." *Perspectives on Psychological Science* 7 (3): 203-220.

Wilson, Tom D. 2000. "Human Information Behavior." *Informing Science* 3 (2): 49-55.

Wilson, Tom D. 1994. "Information needs and uses: fifty years of progress." In *Fifty years of information progress: a Journal of Documentation review*, edited by B.C. Vickery, 15-51. London: Aslib. http://informationr.net/tdw/publ/papers/1994FiftyYears.html.

Wright, Peter. 1987. *Spycatcher.* Toronto: Stoddart.

Yan, Jeff, and Ahmad Salah El Ahmad. 2008. "Usability of CAPTCHAs or usability issues in CAPTCHA design." *Proceedings of the 4th symposium on Usable privacy and security.* New York: ACM. 44-52.

Yang, Ran, Yu Jie Ng, and Arun Vishwanath. 2015. "Do Social Media Privacy Policies Matter? Evaluating the Effects of Familiarity and Privacy Seals on Cognitive Processing." *Proceedings of the 2015 48th Hawaii International Conference on System Sciences.* Washington D.C.: IEEE Computer Society. 3463-3472.

Yee, Ka-Ping. 2002. "User Interaction Design for Secure Systems." *Information and Communications Security.* Springer Berlin Heidelberg. 278-290.

Yost, Jeffrey R. 2007. "A History of Computer Security Standards." In *The History of Information Security: A Comprehensive Handbook*, edited by Karl de Leeuw and Jan Bergstra, 595-621. Amsterdam: Elsevier.

Zimmer, Michael, and Nicholas John Proferes. 2014. "A topology of Twitter research: disciplines, methods, and ethics." *Aslib Journal of Information Management* 66 (3): 250-261.

Zittrain, Jonathan. 2008. *The Future of the Internet and How to Stop It.* New Haven: Yale University Press.

Zuboff, Shoshana. 1984. *In the Age of the Smart Machine: The Future of Work and Power.* New York, New York: Basic Books.

Zwick, Detlev, and Alan Bradshaw. 2014. "Capital's New Commons: Consumer Communities, Marketing and the Work of the Audience inn Communicative Capitalism." In *The Audience Commodity in the Digital Age*, edited by Lee McGuigan and Vincent Manzerolle, 158-172. New York: Peter Lang Publishing.

Appendices

Table 36 - Full List of Tasks and Conditions

Platform	Pre-task	Condition 1	Condition 2	Primary	Secondary	Tertiary	Tertiary	Tertiary
Facebook	*Pre-task*	*Condition 1 (Yes/No)*	*Condition 2 (Yes/No)*	*Primary Authentication*	*Secondary Authentication*	*Tertiary Data Manipulation App*	*Tertiary Client App Clone*	*Tertiary Service & Product App*
Task	First Authentication	Security & Privacy Awareness	Security & Privacy Management	Login to Facebook	Instagram (Android)	dlvr.it (Desktop)	Playbook Facebook Clone (Blackberry)	Angry Birds Friends (Desktop)
Description	Enable third-party platform	Read the user agreement	Customize your security and privacy settings	Post a comment	Follow an Instagram user from the selected list	Post an update to your timeline	Like a post	Invite one or more friends
Google	*Pre-task*	*Condition 1 (Yes/No)*	*Condition 2 (Yes/No)*	*Primary Authentication*	*Secondary Authentication*	*Tertiary Data Manipulation App*	*Tertiary Client App Clone*	*Tertiary Service & Product App*
Task	First Authentication	Security & Privacy Awareness	Security & Privacy Management	Login to Google + (Desktop)	Google Docs (Desktop)	Organizer for Google Docs (Android)	Spark (iOS)	Dropbox (Desktop)
Description	Login and change password	Read the user agreement	Customize your security and privacy settings	Add a skill to your profile	Invite someone to edit a document	Move a document in a new folder.	Adjust your email signature	Respond to an invitation to join a group
Twitter	*Pre-task*	*Condition 1 (Yes/No)*	*Condition 2 (Yes/No)*	*Primary Authentication*	*Secondary Authentication*	*Tertiary Data Manipulation App*	*Tertiary Client App Clone*	*Tertiary Service & Product App*
Task	First Authentication	Security & Privacy Awareness	Security & Privacy Management	Login to Twitter	Vine (desktop)	Hootsuite (iOS)	Talon (Android)	Medium (desktop)
Description	Login and change password	Read the user agreement	Customize your security and privacy settings	Post a tweet	Follow a Vine user from the select list	Retweet a tweet	Favourite a tweet	Post the article of one user to your Twitter account

Table 37 - Potential Participants' Self-Screening Survey

Mobile and Social Networking Literacy Study Eligibility Survey
Hello. Thank you for responding to this call for participants. My name is Hervé Saint-Louis, I am a PhD candidate at the Faculty of Information, at the University of Toronto. This form allows the research team to determine your level of suitability for this study. We seek participants for our study with undisclosed level of familiarity with several mobile and social media platforms. Answer as honestly as possible. There are no right or wrong answers. Reply with an email with the selected answer per question. In your response, please use your real email. 1-Have you used Facebook before? A) Never used B) Used once C) Used in the last three months D) Used frequently E) I don't know 2-Have you used Gmail before? A) Never used B) Used once C) Used in the last three months D) Used frequently E) I don't know 3-Have you used Twitter before? A) Never used B) Used once C) Used in the last three months D) Used frequently E) I don't know 4-I have used Facebook, Gmail, or Twitter on a desktop or laptop computer previously. A) Never used B) Used once C) Used in the last three months D) Used frequently E) I don't know 5-Do you use any of the following apps or services; AngryBirds Friends (through Facebook), Business Organizer for Google Docs (on Android), dlvr.it, Dropbox, Google Forms, Instagram, Medium, Spark, Talon, or Vine? A) Yes B) No 6-Age A) Under 18 B) 18 and above 7-Gender A) Female B) Male 8-I live in the GTA area and can travel to University of Toronto (St. George campus) in downtown Toronto? A) Yes B) No PLEASE DO NOT INSTALL THE FOLLOWING IF YOU WISH TO TAKE PART IN THIS STUDY; AngryBirds Friends (through Facebook), Business Organizer for Google Docs (on Android), dlvr.it, Dropbox, Google Forms, Instagram, Medium, Spark, Talon, Vine. Best regards Hervé Saint-Louis PhD Candidate, Faculty of Information University of Toronto

Table 38 - Participants Demographics

PARTICIPANTS	AGE	AGE RANGE	GENDER	SCENARIO
P01	29	25-34	Male	yes/yes
P02	37	35-44	Male	yes/no
P03	29	25-34	Male	no/yes
P04	58	55-64	Female	no/no
P05	18	18-24	Female	no/no
P06	32	25-34	Male	no/no
P07	N/A	35-44	Female	no/yes
P08	27	25-34	Female	Yes/yes
P09	29	25-34	Male	Yes/yes
P10	27	25-34	Female	Yes/no
P11	68	65+	Female	No/yes
P12	31	25-34	Female	Yes/yes
P13	57	55-64	Female	Yes/no
P14	24	18-24	Male	Yes/no
P15	29	25-34	Male	No/yes
P16	23	18-24	Female	Yes/yes
P17	61	55-64	Male	No/no
P18	24	18-24	Female	Yes/no
P19	23	18-24	Male	No/yes
P20	26	25-34	Male	No/no

Table 39 - Experiment Protocols

September 20, 2016 Protocols

Read these policies, and skim through these presentations before doing the test.

PRE-TASKS

Mental Model Illustration Laptop

a) With the laptop, open the Firefox browser.
b) Search for 'Johnny Bullet comic strip' in any of the search bars.
c) Go to the comic strip homepage hosted by the site ComicBookBin.com
d) Click on the large image of the comic strip.
e) Read the comic strip.
f) Add a bookmark to the page (with the keyboard, click on crtl+D if you do not know how to add a bookmark).
g) Close the browser.
h) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings your interaction with the device, the software, and the website. Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Repeat Mental Model Illustration Android

a) Pick up the Android tablet and flip it in horizontal mode. Wake up the tablet.
b) Search for 'Johnny Bullet comic strip' using a browser by clicking the Google icon in the top left corner or the search box at the top of the home screen.
c) Go to the comic strip homepage hosted by the site ComicBookBin.com
d) Click on the large image of the comic strip.
e) Click the first page button above the comic strip.
f) Leave a comment about the comic strip in the Johnny Bullet #1 without creating or log into an account.
g) Exit the page.
h) Close the browser.
i) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings your interaction with the device, the software, and the website. Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Repeat Mental Model Illustration Playbook

a) Pick up the Playbook tablet and flip it in horizontal mode. Wake up the tablet.
b) Search for 'Johnny Bullet comic strip' in the Google search box at the top of the home screen.
c) Go to the comic strip homepage hosted by the site ComicBookBin.com
d) Click on the large image of the comic strip.
e) Click the previous page button above the comic strip.
f) Leave a comment about the comic strip in the Johnny Bullet #1 without creating or log into an account.
g) Exit the page.
h) Close the browser.

i) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings your interaction with the device, the software, and the website. Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Repeat Mental Model Illustration iPad

a) Pick up the Playbook tablet and flip it in horizontal mode.
b) Search for 'Johnny Bullet comic strip' in the Google search box at the top of the home screen.
c) Go to the comic strip homepage hosted by the site ComicBookBin.com
d) Click on the large image of the comic strip.
e) Leave a comment about the comic strip in the current Johnny Bullet without creating or login into an account.
f) Exit the page.
g) Close the browser.
h) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings your interaction with the device, the software, and the website. Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

1) Pre-Task: Facebook

a) Log into your Facebook account

b) Find the Settings options in the top right corner under the inverted triangle.

c) Once you clicked on Settings, find the Apps icon on the left side of the screen and click on it.

d) Find the "Apps, Websites and Plug-ins" and verify if your option is disabled or not.

e) If the option is disabled, please click on the "Edit" button to enable the platform features of Facebook. We need this to be enabled in order to perform the tests.

f) Log out of Facebook.

1) Pre-Task: Twitter

a) Using the laptop computer, log into your Twitter account.

b) Find your profile pic in the top right corner and click on it. You may or may not have a personal picture there. In such a case, the default pic will appear.

c) Select the "Settings" option from the drop down list.

d) Find the "Password" option. You will change your password options.

e) Enter your current password into the 'Current Password' field.

f) Take the Android tablet and open the Random Password Generator app.

g) Using the Random Password Generator app on the Android device, generate a new password for your Twitter account.

h) Transcribe the new password on a sheet of paper to avoid losing it by mistake.

i) Transcribe the new password generated by the Password Generator app into the 'New Password' field in the Twitter Password settings on the laptop computer.

j) Transcribe the new password generated by the Password Generator app into the 'Verify Password' field in the Twitter Password settings on the laptop computer.

k) Save the changes.

l) The screen has now switched and includes two options, 'Review applications' and 'no thanks'.

m) Click on Review applications.

n) Verify that the Hootsuite third party apps is not enabled. If it is, revoke its access.

o) Verify that the Medium third party apps is not enabled. If it is, revoke its access.

p) Verify that the Talon third party apps is not enabled. If it is, revoke its access.

q) Verify that the Vine third party apps is not enabled. If it is, revoke its access.

r) Click on your profile pic in the top right corner and log out of Twitter.

1) Pre-Task: Google

a) Using the laptop computer, log into your Google Drive Account.

b) Click on the 'NEW' button in the top left corner.

c) Click on the folder icon within the drop-down menu.

d) Create a new folder called 'My Study'.

e) Click on the 'My Study' folder to access it.

f) With the mouse, right click to make the contextual menu appear.

g) Click on the Google Docs Button.

h) Create a new Doc file. Type in the word "Hello" in the top left corner to name the file.

j) Go back to the My Study folder.

j) Create a new folder inside of the 'My Study' folder. Name this folder 'Results'.

k) Sign out of Google.

INTERVENTIONS

Facebook

2) Intervention 1

a) To speed up the usability test, we invite you to read some Facebook privacy and security policies ahead of time.

3) Intervention 2

a) Login to Facebook

b) To speed up the usability test, we suggest that you adjust your Facebook privacy and security options as you see fit, before we start the evaluation, since we won't have time to do so later.

c) Click on the triangle in the top right menu.

d) Click Settings and then adjust your privacy and security settings. You can find the privacy and security options in the top left side.

e) Log out of Facebook.

Twitter

2) Intervention 1

a) To speed up the usability test, we invite you to read some Twitter privacy and security policies ahead of time.

3) Intervention 2

a) To speed up the usability test, we suggest that you adjust your Twitter privacy and security options as you see fit, before we start the evaluation, since we won't have time to do so later. Login, adjust your settings, save them and then log out.

b) To adjust your privacy and security settings, click on your profile icon in the top right corner.

c) Click on Settings.

d) Click on the Security and privacy tab and then adjust your settings as you deem fit.

e) Log out of Twitter by clicking your profile icon in the top right corner then select log out.

Google

2) Intervention 1

a) To speed up the usability test, we invite you to read some Google privacy and security policies ahead of time.

3) Intervention 2

a) To speed up the usability test, we suggest that you adjust your Google privacy and security options as you see fit, before we start the evaluation, since we won't have time to do so later. Here is how to do this.

b) Log into your Google Account.

c) Click on the top right icon and press the My Account button.

d) To adjust your security options, click on the Sign-in & Security option in the left column of the screen.

e) To adjust your privacy options, click on the Personal info & Privacy options.

f) When done, click on the top right icon and press the sign out button.

TASKS

Task 1

a) Randomized Task #1-Facebook Primary Authentication

i) Using the laptop computer, login to Facebook.

ii) Post a comment on your timeline.

iii) Log out of Facebook. Exit the browser.

iv) Mental Model Rich Picture

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Facebook? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 2

b) Randomized Task #2-Instagram Secondary Authentication through Facebook

i) Using the laptop computer, login to Instagram using the log in option for users with Facebook accounts.

ii) After browsing possibilities, follow an Instagram user of your choice.

iii) Log out of Instagram. To do so, click on the profile icon. Then press on the three dots. Then click log out.

iv) Mental Model Rich Picture.

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Instagram and Facebook? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 3

c) Randomized Task #3-AngryBirds Friends Tertiary Authentication through Facebook

i) Using the laptop computer, login to Facebook.

ii) Search for the AngryBirds Friends app.

iii) Install and or Play the AngryBirds Friends app.

iv) Play the first level of the game for about one minute or two.

v) Whether you won or not logout of Facebook.

vi) Mental Model Rich Picture

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with AngryBirds Friends and Facebook? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 4

d) Randomized Task #4-dlver.it Tertiary Authentication through Facebook

i) Using the laptop computer, login to dlvr.it using the Sign Up option for users with Facebook accounts. Click yes to confirm your email.

ii) After browsing possibilities, add the following RSS feed as a source to your dlvr.it account http://www.comicbookbin.com/rss.xml. To do so, copy the URL of the feed from the next tab.

iii) Paste the URL of the feed into the RSS feed field.

iv) Then, Press the Plus button.

v) Sign out of dlvr.it.

vi) Mental Model Rich Picture.

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with dlvr.it and Facebook? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 5

e) Randomized Task #5-Facebook clone client Tertiary Authentication through Facebook

i) Click on the power button at the top of the Playbook to end the sleep mode of the device.

ii) Using the BlackBerry Playbook tablet, launch the Facebook app.

iii) Use your Facebook account profile to login to the Facebook app on the Playbook tablet.

iv) Find any post from your network of friends, family, colleagues, or acquaintances, and like it.

v) Put the tablet to sleep by clicking the power button on top of the device.

vi) Mental Model Rich Picture.

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with the Playbook Facebook app and Facebook? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 6

a) Randomized Task #1-Twitter Primary Authentication

i) Using the laptop computer, login to Twitter.

ii) Post a comment on your Twitter feed.

iii) Log out of Twitter

iv) Mental Model Rich Picture

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Twitter? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 7

b) Randomized Task #2-Vine Secondary Authentication through Twitter

i) Using the Android tablet, launch the Vine app.

ii) Use your Twitter account profile to create a new Vine account through the Android tablet. Skip the profile icon option.

iii) Say no to access your contacts

iv) Skip to next

v) In the search bar, search for 'Derek Salvator'.

vi) After watching a few of Derek Salvator's vines with music enabled, put a comment if you want to.

vii) Shut Vine.

viii) Mental Model Rich Picture.

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Vine and Twitter? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 8

c) Randomized Task #3-Hootsuite Tertiary Authentication through Twitter

i) Using the iPad, launch the Hootsuite app.

ii) Use your Twitter account profile to sign into Hootsuite.

iii) Add your Twitter account to Hootsuite as the default social media account being monitored. There is no need to add another social network.

iv) Retweet a tweet posted by anyone.

v) Favourite (like) one of your follower or a person you follow's tweet.

vi) Exit Hootsuite.

vii) Mental Model Rich Picture

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Hootsuite and Twitter? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 9

d) Randomized Task #4-Talon Tertiary Authentication through Twitter

i) Using the Android tablet, launch the Talon app.

ii) Use your Twitter account profile to log into Talon.

iii) Authorize Talon from having access to your Twitter account.

iv) Post a tweet

v) Logout of Talon.

vi) Mental Model Rich Picture.

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Talon and Twitter? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 10

e) Randomized Task #5-Medium Tertiary Authentication through Twitter

i) Using the laptop computer, login to medium.com using the Sign Up option for users with Twitter accounts.

ii) Pick a topic. After browsing a few stories, follow one or two users.

iii) Log out of Medium.

iv) Mental Model Rich Picture.

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Medium and Twitter? Add new icons and symbols if you require. There are no right or wrong answers.

Task 11

a) Randomized Task #1-Google Primary Authentication

i) Using the laptop computer, login to Google.

ii) Click on the bell icon in the top right corner of the screen.

iii) A pop up will open. Click on the gear icon in the top left corner of the pop up.

iv) Adjust your notifications settings by checking or unchecking options for apps. If there are no options shut the menu by clicking outside of the pop up.

v) Log out of Google by clicking the top right pic and select sign out.

vi) Mental Model Rich Picture

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Google? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 12

b) Randomized Task #2-Google Docs (Forms) Secondary Authentication through Docs

i) Using the laptop computer, login to Google Forms.

ii) Find the 'Start a new form' option and create a new 'Party Invite' using the template.

iii) Adjust the template to your personal preferences.

iv) When done, click on the eye icon in the top right menu to preview your party invite.

v) When done, shut the party invite preview tab.

vi) Back in the party invite template, click the top left arrow to exit the template.

vii) Log out of Google Forms.

viii) Mental Model Rich Picture.

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Forms and Google? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 13

c) Randomized Task #3-Spark Tertiary Authentication through Google

i) Using the iPad, launch the Spark app.

ii) Click on login to connect your Google account to Spark by clicking on the Google logo. Click OK for "I understand the notifications".

iii) Enter your Gmail address in the first field, then click next.

iv) Enter your Gmail password in the first field, then click sign in.

v) Click Allow Spark to access your email, to display your email address, and to display information based on your profile.

vi) Click on the green DONE button to finish the set up.

vii) Click 'done' to remove the prompt to add a second account.

viii) Click on the bottom right blue button to start an email.

ix) Write an email to hcitoon@gmail.com to let the lead investigator know that you have completed the process.

x) Exit Spark.

xi) Mental Model Rich Picture

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Spark and Google? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task 14

d) Randomized Task #4-Dropbox Tertiary Authentication through Google

i) Using the laptop computer, sign in Dropbox using the Google Account option.

ii) Allow Dropbox to have access to your Google Account.

iii) Choose a new password.

iv) Type in the bot check password.

v) Pick a personal or work account.

vi) Accept to download Dropbox.

vii) Shut down Firefox without installing the file.

viii) Mental Model Rich Picture.

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Dropbox and Google? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

Task15

e) Randomized Task #5-Organizer for Google Docs Tertiary Authentication through Google

i) Using the Android tablet, launch the Organizer for Google Docs app.

ii) Choose to connect your Google account to Organizer by clicking on the Google logo.

iii) Enter your Gmail address in the first field, then click next.

iv) Enter your Gmail password in the first field, then click Connect.

v) Authorize Organizer from accessing your files etc., to display your email address, and to display information based on your profile. Do not back up any data on the device.

vi) From Organizer, Move the "Hello" document from the 'My Study' folder into the 'Results' folder.

viii) Exit Organizer for Google.

ix) Mental Model Rich Picture.

(1) Using the pre-printed icons as building blocks and the drawing tools at your disposal, explain through drawings how you interacted with Organizer and Google? Add new icons and symbols if you require. There are no right or wrong answers. You have two minutes to complete this task.

POST TEST

5) Post-Task Facebook (the post-task occurs after all tasks on Facebook, Google, and Twitter are completed)

a) Using the laptop computer, log into your Facebook account

b) Find the Settings options in the top right corner under the inverted triangle.

c) Once you clicked on Settings, find the Apps icon on the left side of the screen and click on it.

d) Find the "Apps, Websites and Plug-ins" and verify if your option is disabled or not.

e) Since we asked you to enable the option, we will help you disable it if you wish.

f) Do you wish to keep the option enabled or disabled?

g) If you choose to disable the option, please click on the "Edit" button to disable the platform features of Facebook.

h) Log out of Facebook.

5) Post-Task Twitter (the post-task occurs after all tasks on Facebook, Google, and Twitter are completed)

a) Using the laptop computer, log into your Twitter account

b) Find your profile pic in the top right corner and click on it.

c) Select the "Settings" option from the drop-down list.

d) Find the "Password" option. You will change your password options.

e) If you wish to, reset your password to something else.

f) Save the changes and or/ go to the Apps tab

g) The screen has now switched and includes two options, 'Review applications' and 'no thanks'. And / or the Apps tab.

h) Click on Review applications. And or / Apps tab

i) Revoke the access of any app that you do not want to continue using, including Hootsuite, Medium, Talon or Vine.

j) Click on your profile pic in the top right corner and log out of Twitter.

5) Post Test Google (the post-task occurs after all tasks on Facebook, Google, and Twitter are completed)

a) Using the laptop computer, log into your Google Drive account

b) Find the My Study folder.

c) Right click to remove the folder.

d) Remove the My study folder.

e) Sign out of Google.

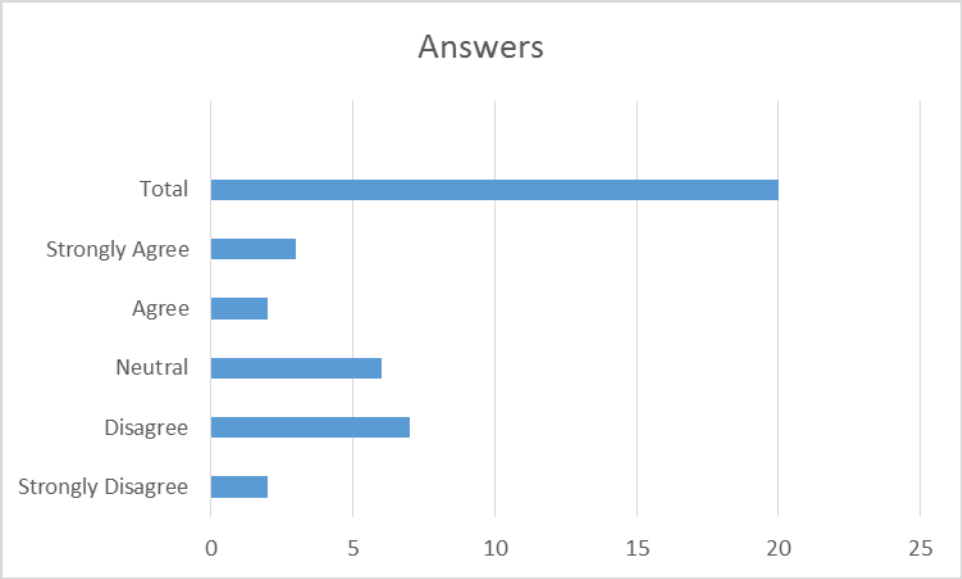

Figure 35 - Question 1 Likert Scale Results

Table 40 - Q1 Mann-Whitney Test

Ranks

	var2	N	Mean Rank	Sum of Ranks
Q1	0	10	10.65	106.50
	1	10	10.35	103.50
	Total	20		

Test Statistics[a]

	Q1
Mann-Whitney U	48.500
Wilcoxon W	103.500
Z	-.118
Asymp. Sig. (2-tailed)	.906
Exact Sig. [2*(1-tailed Sig.)]	.912[b]

a. Grouping Variable: var2

b. Not corrected for ties.

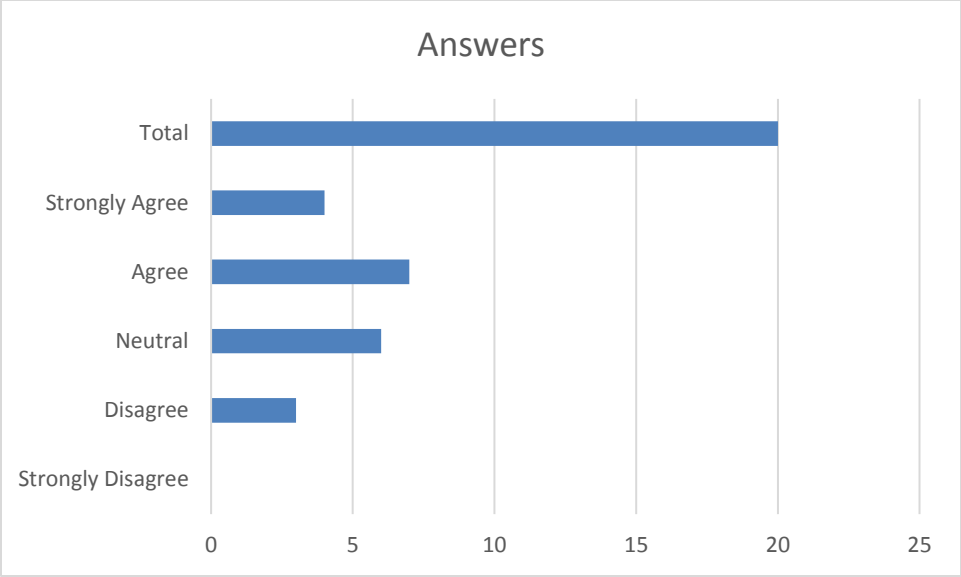

Figure 36 - Question 2 Likert Scale Results

Table 41 - Q2 Mann-Whitney Test

Ranks

	var2	N	Mean Rank	Sum of Ranks
Q2	0	10	11.15	111.50
	1	10	9.85	98.50
	Total	20		

Test Statistics[a]

	Q2
Mann-Whitney U	43.500
Wilcoxon W	98.500
Z	-.512
Asymp. Sig. (2-tailed)	.609
Exact Sig. [2*(1-tailed Sig.)]	.631[b]

a. Grouping Variable: var2

b. Not corrected for ties.

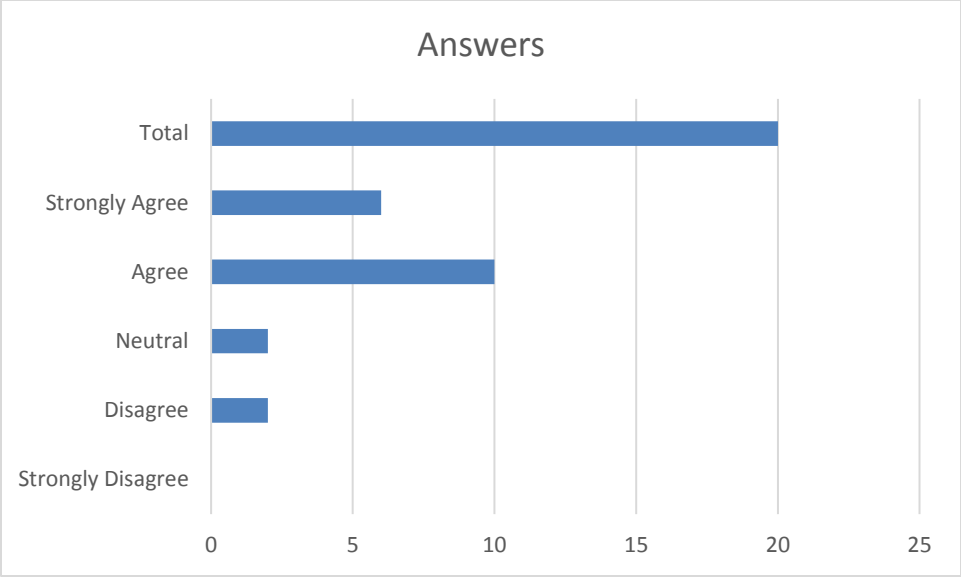

Figure 37 - Question 3 Likert Scale Results

Table 42 - Q3 Mann-Whitney Test

Ranks

	var2	N	Mean Rank	Sum of Ranks
Q3	0	10	9.70	97.00
	1	10	11.30	113.00
	Total	20		

Test Statistics[a]

	Q3
Mann-Whitney U	42.000
Wilcoxon W	97.000
Z	-.657
Asymp. Sig. (2-tailed)	.511
Exact Sig. [2*(1-tailed Sig.)]	.579[b]

a. Grouping Variable: var2

b. Not corrected for ties.

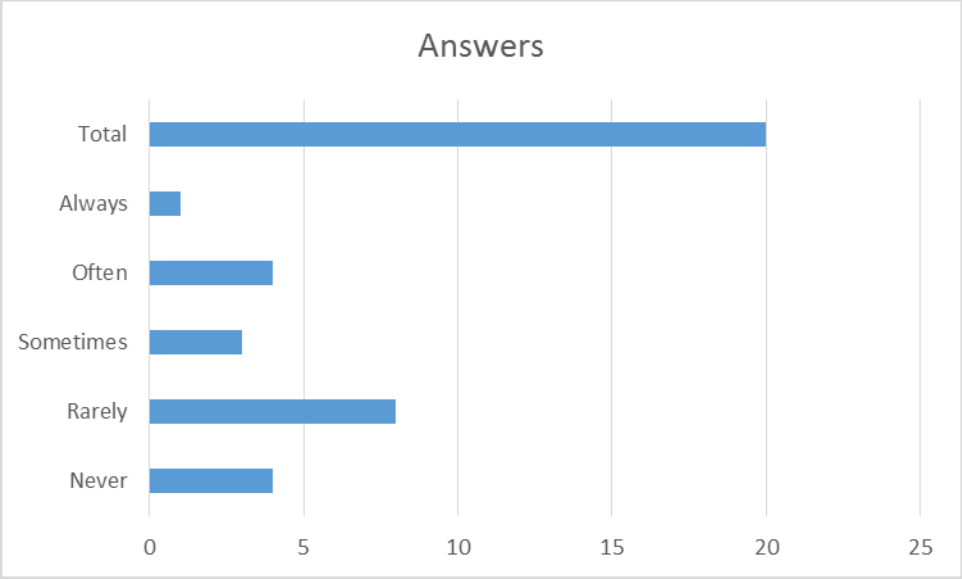

Figure 38 - Question 5 Likert Scale Results

Table 43 – Q5 Mann-Whitney Test

Ranks

	var2	N	Mean Rank	Sum of Ranks
Q5	0	10	10.45	104.50
	1	10	10.55	105.50
	Total	20		

Test Statistics[a]

	Q5
Mann-Whitney U	49.500
Wilcoxon W	104.500
Z	-.039
Asymp. Sig. (2-tailed)	.969
Exact Sig. [2*(1-tailed Sig.)]	.971[b]

a. Grouping Variable: var2

b. Not corrected for ties.

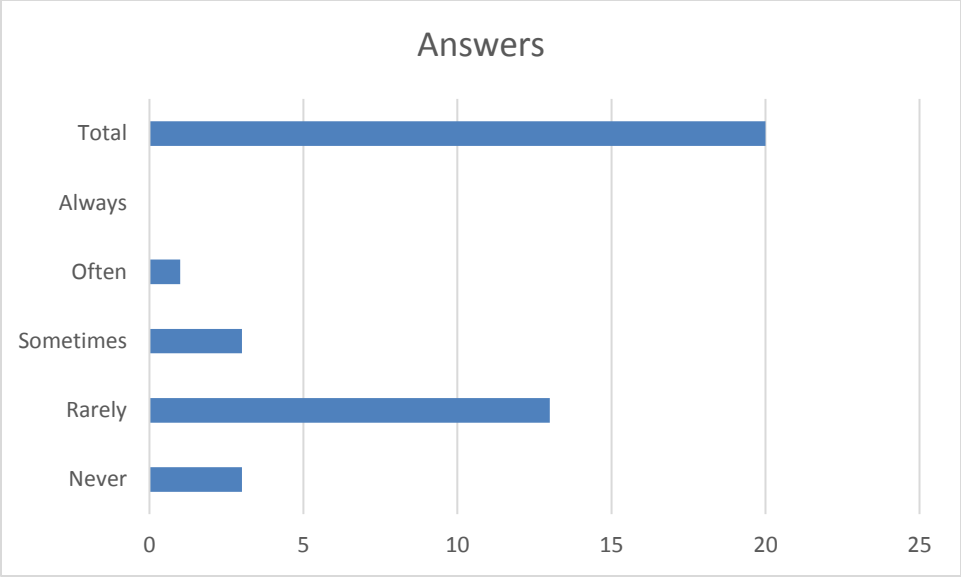

Figure 39 - Question 6 Likert Scale Results

Table 44 – Q6 Mann-Whitney Test

Ranks

	var2	N	Mean Rank	Sum of Ranks
Q6	0	10	9.20	92.00
	1	10	11.80	118.00
	Total	20		

Test Statistics[a]

	Q6
Mann-Whitney U	37.000
Wilcoxon W	92.000
Z	-1.158
Asymp. Sig. (2-tailed)	.247
Exact Sig. [2*(1-tailed Sig.)]	.353[b]

a. Grouping Variable: var2

b. Not corrected for ties.

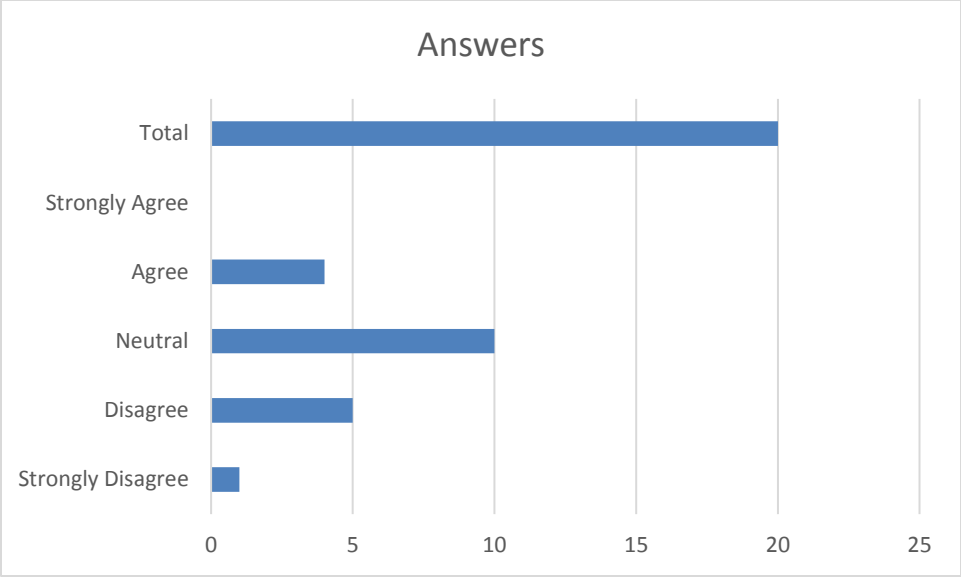

Figure 40 - Question 8 Likert Scale Results

Table 45 – Q8 Mann-Whitney Test

Ranks

	var2	N	Mean Rank	Sum of Ranks
Q8	0	10	11.35	113.50
	1	10	9.65	96.50
	Total	20		

Test Statistics[a]

	Q8
Mann-Whitney U	41.500
Wilcoxon W	96.500
Z	-.696
Asymp. Sig. (2-tailed)	.487
Exact Sig. [2*(1-tailed Sig.)]	.529[b]

a. Grouping Variable: var2

b. Not corrected for ties.

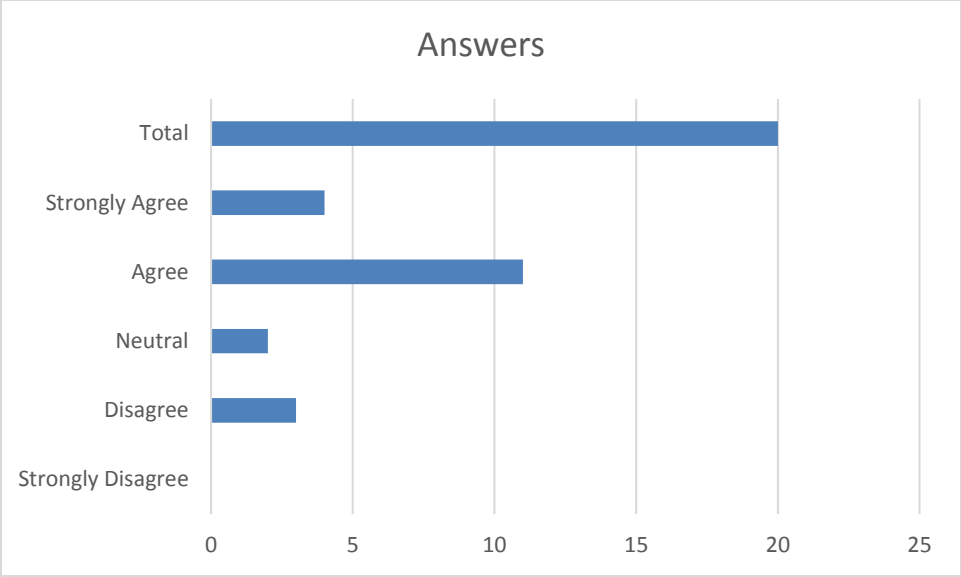

Figure 41 - Question 4 Likert Scale Results

Table 46 – Q4 Mann-Whitney Test

Ranks

	var3	N	Mean Rank	Sum of Ranks
Q4	0	12	10.83	130.00
	1	8	10.00	80.00
	Total	20		

Test Statistics[a]

	Q4
Mann-Whitney U	44.000
Wilcoxon W	80.000
Z	-.340
Asymp. Sig. (2-tailed)	.734
Exact Sig. [2*(1-tailed Sig.)]	.792[b]

a. Grouping Variable: var3

b. Not corrected for ties.

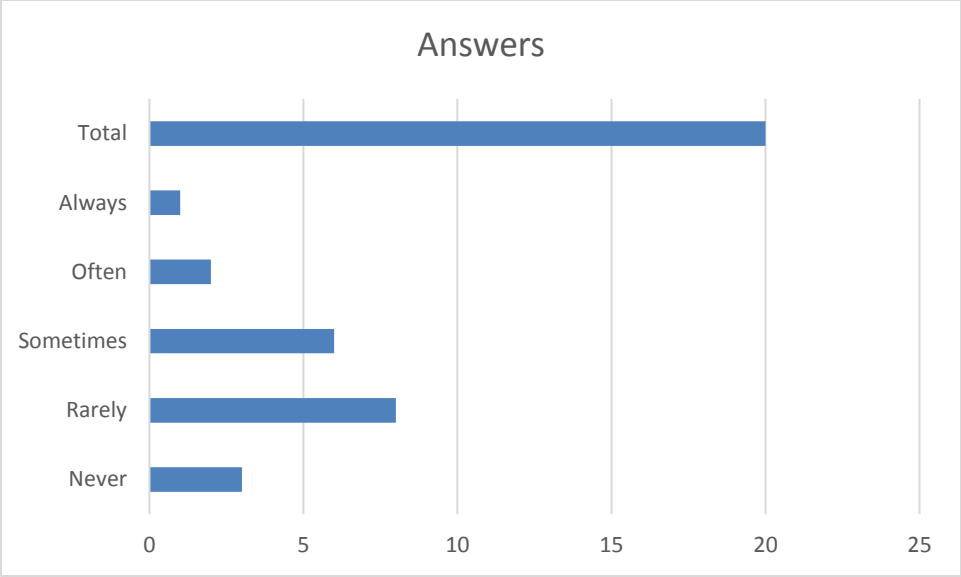

Figure 42 - Question 7 Likert Scale Results

Table 47 – Q7 Mann-Whitney Test

Ranks

	var3	N	Mean Rank	Sum of Ranks
Q7	0	12	11.67	140.00
	1	8	8.75	70.00
	Total	20		

Test Statistics[a]

	Q7
Mann-Whitney U	34.000
Wilcoxon W	70.000
Z	-1.134
Asymp. Sig. (2-tailed)	.257
Exact Sig. [2*(1-tailed Sig.)]	.305[b]

a. Grouping Variable: var3

b. Not corrected for ties.

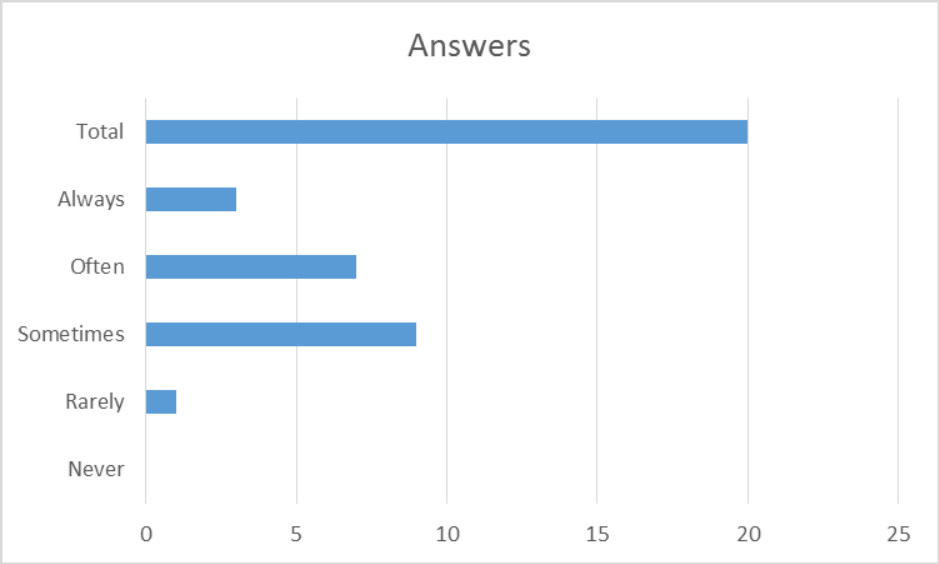

Figure 43 - Question 9 Likert Scale Results

Table 48 – Q9 Mann-Whitney Test

Ranks

	var3	N	Mean Rank	Sum of Ranks
Q9	0	12	8.67	104.00
	1	8	13.25	106.00
	Total	20		

Test Statistics[a]

	Q9
Mann-Whitney U	26.000
Wilcoxon W	104.000
Z	-1.825
Asymp. Sig. (2-tailed)	.068
Exact Sig. [2*(1-tailed Sig.)]	.098[b]

a. Grouping Variable: var3

b. Not corrected for ties.

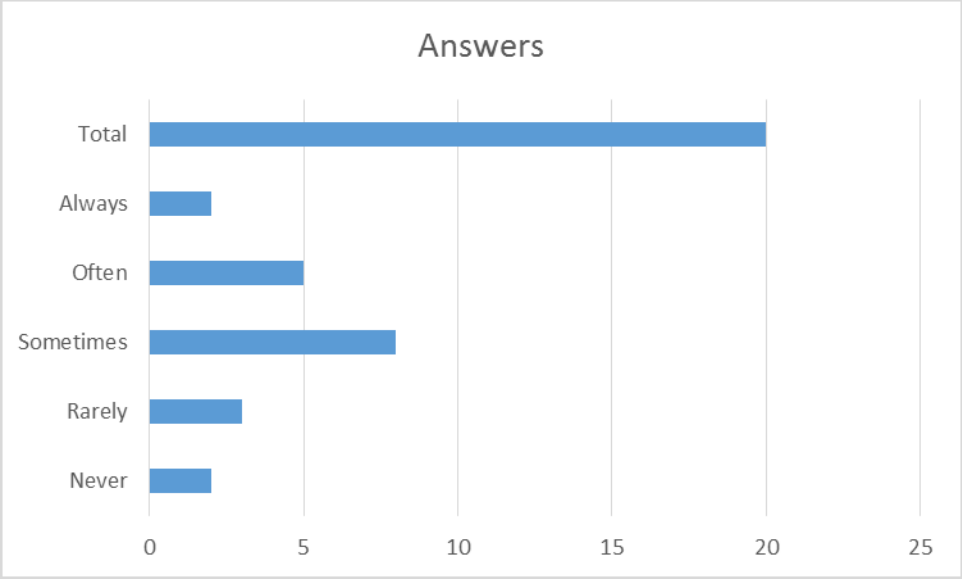

Figure 44 - Question 10 Likert Scale Results

Table 49 - Q10 Mann-Whitney Test

Ranks

	var3	N	Mean Rank	Sum of Ranks
Q10	0	12	8.63	103.50
	1	8	13.31	106.50
	Total	20		

Test Statistics[a]

	Q10
Mann-Whitney U	25.500
Wilcoxon W	103.500
Z	-1.812
Asymp. Sig. (2-tailed)	.070
Exact Sig. [2*(1-tailed Sig.)]	.082[b]

a. Grouping Variable: var3

b. Not corrected for ties.

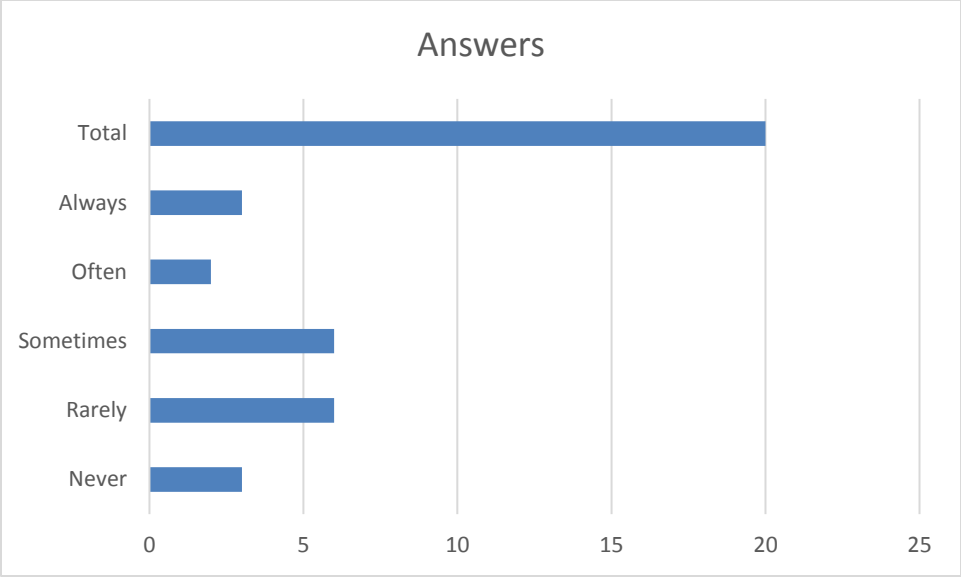

Figure 45 - Question 11 Likert Scale Results

Table 50 – Q11 Mann-Whitney Test

Ranks

	var3	N	Mean Rank	Sum of Ranks
Q11	0	12	10.21	122.50
	1	8	10.94	87.50
	Total	20		

Test Statistics[a]

	Q11
Mann-Whitney U	44.500
Wilcoxon W	122.500
Z	-.278
Asymp. Sig. (2-tailed)	.781
Exact Sig. [2*(1-tailed Sig.)]	.792[b]

a. Grouping Variable: var3

b. Not corrected for ties.

Table 51 - Latin Square

TEST & CONTROL GROUPS	MALE	FEMALE	TOTAL
YES YES	2	3	5
YES NO	2	3	5

NO YES	3	2	5
NO NO	3	2	5
TOTAL	10	10	20
CONDITION 1	Participants' perceptions of security and confidentiality with tertiary authentication.		
CONDITION 2	Participants' control and management of security and confidentiality with tertiary authentication.		

Table 52 - Types of Authentication

AUTHENTICATION	PLATFORM MAPPING	APP MAPPING
PRIMARY AUTHENTICATION	Facebook	(desktop)
SECONDARY AUTHENTICATION	Facebook	Instagram (Android)
TERTIARY AUTHENTICATION	Facebook	dlvr.it (desktop)
TERTIARY AUTHENTICATION	Facebook	Angry Birds Friends (desktop)
TERTIARY AUTHENTICATION	Facebook	Facebook client (Blackberry Playbook tablet)
PRIMARY AUTHENTICATION	Google	(desktop)
SECONDARY AUTHENTICATION	Google	Google Forms (Desktop)
TERTIARY AUTHENTICATION	Google	Business Organizer (Android)
TERTIARY AUTHENTICATION	Google	Sparks (iOS)
TERTIARY AUTHENTICATION	Google	Dropbox (desktop)
PRIMARY AUTHENTICATION	Twitter	(desktop)
SECONDARY AUTHENTICATION	Twitter	Vine (desktop)
TERTIARY AUTHENTICATION	Twitter	Hootsuite (iOS)
TERTIARY AUTHENTICATION	Twitter	Talon (Android)
TERTIARY AUTHENTICATION	Twitter	Medium (desktop)

Mobile and Social Networking Literacy Study

Adults between 18+ needed

Requirements

- 18 +
- You have a Facebook account
- You have a Google account
- You have a Twitter account
- You are not a Instagram, Medium, Vine, and Google Forms user

The Study

The experiment lasts between 2-3 hours.

Selected participants receive a compensation.

Participants must be available to travel to the University of Toronto's downtown campus (St. George campus) during July and October 2016.

Interested candidates should send an email at herve.saint.louis@mail.utoronto.ca

Use the title "Mobile and Social Networking Literacy Study" in your email

Please include your

- Full name
- Gender
- Email
- Age
- Telephone number

Researcher: Hervé Saint-Louis
PhD Candidate, Faculty of Information

Supervisor: Professor Rhonda McEwen
Faculty of Information, University of Toronto
Approved by the University of Toronto
Research Ethics Board

UNIVERSITY OF TORONTO
FACULTY OF INFORMATION

Figure 46 - Recruitment Poster

Informed Consent Form 1

Consent Form

I agree to participate in the study ("An evaluation of user interactions with third party apps") that evaluates user interactions of tertiary apps used with primary social media platforms. This study is being conducted by doctoral candidate Hervé Saint-Louis (Faculty of Information at the University of Toronto).
I understand that my participation is entirely voluntary. The following points have been explained to me:
1. The goal of this study is to evaluate the performance, the perceptions, and the implications of tertiary interactions with a desktop, mobile and tablet-based primary social media platforms used by users. I understand that I will participate in the following experiment:
i. I will interact with a desktop, mobile and tablet-based social media platforms and third party applications accessed through the primary platforms as instructed by the experimenter.
ii. I will perform a series of tasks requiring me to draw the mental models of my interactions with the primary platforms and the tertiary apps.
iii. The tasks and usage of the mental model drawings will be explained to me by the experimenter.

2. Upon completion of the study, I will receive a financial compensation of $20 in the form of a Chapters-Indigo gift card.

3. I will use my personal accounts with the following platforms; Facebook, Google and Twitter; to perform the interactions with the tertiary apps in the experiment.

4. My personal data on Facebook, Google, and Twitter will not be recorded as part of this experiment and will not be associated with my name or identity. My personal data on Facebook, Google, and Twitter will not be released publicly and will be destroyed upon completion of the analysis of data collected in this experiment or after 36 months after the completion of this experiment, whichever will occur first. Any data retained about my accounts on Facebook, Google, and Twitter will be stored securely and password-protected on a server maintained by the Faculty of Information, with only the experimenter having access to it.

5. I understand that data will be automatically collected on the provided device that captures my entire interaction with the applications, such as time to complete tasks, button pressed, and other interactions with the interface of the application.

6. I understand that any data collected (on-device logs, audio likeness, or answers to questionnaires) will not be associated with my name, but an anonymous user ID will be used instead. This data will not be released publicly but will be incorporated anonymously and in aggregated form in

UNIVERSITY OF TORONTO
FACULTY OF INFORMATION

Figure 47 - Consent Form Page 1

Informed Consent Form 2

reports and statistical analyses.

7. The investigator does not foresee any risk greater than those experienced when interacting with other tablet-based applications.

8. I understand that this experiment is not testing or evaluating me in any way or form; rather, by performing the tasks required here I am helping evaluate the software interface being developed.

9. I understand that I may withdraw from the study at any time after signing the consent form, and receive the entire compensation. The ability to withdraw (including withdrawing any data collected) ceases once I will leave the location of the study upon completion of my participation in the study.

10. I understand that I will receive a copy of this consent form.

11. The experimenter will answer additional questions about the goals of the experiment upon its completion. If you have any questions about the study, please contact me (Hervé Saint-Louis) by phone at 1-416-578-7502 or by email at herve.saint.louis@mail.utoronto.ca.

Further questions about the rights of participants in the study can be directed to the University of Toronto Office of Research Ethics by phone (416) 946-3273 or by email at ethics.review@utoronto.ca. You can also contact my supervisor Professor Rhonda McEwen by phone at 1-416-301-3181 or by email at rhonda.mcewen@utoronto.ca.

This research study may be reviewed for quality assurance to ensure that the required laws and guidelines are followed. If this study is chosen for review, a representative of the Human Research Ethics Program may access the study and consent materials as part of the review process. Information accessed by the Human Research Ethics Program will be upheld to the same level of confidentiality stated by the researcher.

12. Upon completion of this experiment, I will receive an explanation about the rationale and predictions underlying this experiment.

Date

Participant's printed name | Participant's signature

Date

Experimenter name | Experimenter signature

UNIVERSITY OF TORONTO
FACULTY OF INFORMATION

Figure 48 - Consent Form Page 2

Table 53- File Name Protocol

FILE NAME PROTOCOL	
EXAMPLE	p01-02task01a.jpg
PARTICIPANT	p01 (participant 01)
ORDER OF THE SHOT PER SESSION	02
TASK NUMBER	task01
INSTANCE OF THE SHOT PER TASK	a
FILE EXTENSION	.jpg

Table 54- Shots per Participants

SHOTS PER PARTICIPANTS	
PARTICIPANTS	Shots Taken
P 1	35
P 2	36
P 3	33
P 4	31
P 5	30
P 6	44
P 7	34
P 8	33
P 9	34
P 10	43
P 11	34
P 12	35
P 13	43
P 14	35
P 15	47
P 16	53
P 17	45
P 18	53
P 19	48
P 20	54
TOTAL	800

Table 55 – Coders' Profiles

CODERS	FACULTY	EXPERTISE	DEGREE PURSUED
CODER 1	University of Toronto Civil engineering	Water Management	Master's degree
CODER 2	Toronto School of Theology	Divinity	Master's degree
CODER 3	University of Toronto Chemical Engineering	Industrial Water Treatment	Master's degree
CODER 4	University of Toronto Information	Platform Studies	PhD degree

Table 56 - Qualitative Summary of Participant's Diagrammatic Representations

Participants	*Diagrammatic Representation Summaries*
P 1	Once the participant figured out what was happening, he used the same interaction mental model as the basis of his entire work. He particularly paid attention to his personal information and used a key icon to describe encryption processes. He separated the hardware from the platforms when depicting tablets. He did not depict his tasks in detail. This participant has a high level of privacy literacy as he works in some capacity in a research environment exploring privacy issues.
P 2	Often places the primary app as the first one before accessing the third or second party app.
P 3	Does not describes tasks nor access rights processes often.
P 4	It appears that the participant uses the email icon as a stand in for identity or log in. Superficial tasks descriptions. As she had to close the browser, this may explain why the Firefox icon is represented after the Dropbox one. Does not use a step by step way representation of mental models.
P 5	The order that the participant used the tertiary, secondary and primary app was not consistent at first look, but one has to understand what she was interacting with well before determining that it was not consistent according to her perceptions. Did she have an Instagram account before she started the study? This would be the only tertiary/secondary authentication case that differs from the other ones where the primary app was used first.
P 6	The participant does not use platforms and devices as sites of interaction. However, tasks are described further, and logouts are also mentioned.
P 7	The participant does not display the platforms and devices very often as sites of interaction but seems aware of them as they appear in the logouts. The participant also relies on the profile icon when depicting logouts. The tasks are detailed and there is often an awareness of access rights.
P 8	This participant did not remark on authentication much. Tasks are explained in simple terms. Sites of interaction are sometimes mentioned, sometimes not at all. Often, there was a pair of icons for the site of interaction detailing both the site, like a laptop and the actions performed there, like a mouse.
P 9	The participant does note exits at the end of tasks performed. Tasks are often documented.
P 10	The participant often depicts several primary authentication options in models instead of just focusing on the platform selected. Sites of interaction, and tasks are detailed. Uses many paired icons for sites of interaction. Sometimes the laptop leads to parallel paths which still branch in.
P 11	This participant prefers depicting points of interaction instead of tasks performed within these points of interaction. Simple diagrams that hint at log in but indirectly.

P 12	The participant figured out what the study was about and that she did not have to complete all of the tasks. Thus she proceeded to deny as many of the tertiary and secondary authentication as she could. However, she did not fully understand authentications done through clients and allowed some of them. As has been used several times by other participants, the mouse and keyboard connect to the laptop at the root of the path. They are to be considered as devices parts of the site of interaction. The laptop itself, and then the Internet icon which is also used frequently are sites of interaction.
P 13	The participant details tasks at sites of operation carefully. There is one error in icons used in TASK 2. Sites of interaction are well explained too.
P 14	The participant relies on groups of icons and diagrams featuring additions to describe the tasks happening within sites of interaction. Often, the checkmark represents task completion.
P 15	This participant is well aware of access rights and features them well. Devices, browsers and apps often form a group which becomes the site of interaction from which all tasks/actions/operations proceed from. The log out or shutting the app is often represented.
P 16	By clearly separating and labelling the Wi-Fi icon as a site of interaction and differentiating the login from the verification, the participant demonstrated the difference between a site of interaction and a task performed at a site of interaction. Paired groups, such as the profile icon and one of the primary apps are site of interactions where tasks are about to happen. The verification is a task, not a site of interaction. There is an evolution of the mental models used by the participant trying to optimize the icons used in the representation. Yet, the evolution is not a departure or change of the mental models but an optimization of the resources used to describe the tasks.
P 17	The participant uses the icons in full sentences as symbols depicting specific words. So the representation of the mental models is task and action based. Even sites of interaction are represented as being part of actions performed. Often, the participant talks about logouts and shutting tablet-based apps. This does not happen in reality. Other times the participant describes opening the tablet and then the app. But the tablets were always handed to participants with the apps loaded. Web pages were also loaded. The participant has created an idealized version of the interaction where some of the steps were not really performed in practice, but were in theory.
P 18	This participant expressed many of her mental models through artistic illustrations many of which addressed issues not specifically related to authentication. Yet the symbolic representation of the exchange between primary, secondary, and tertiary apps is compelling.
P 19	This participant uses hardware icons such as the keyboard and the mouse economically, connecting them to multiple sites of interaction to convey different tasks being performed by participants. The participant uses the Internet icon often as a site of interaction, understanding that operations are always occurring over that network.
P 20	Participant does not describe tasks in details but does describe points of interactions in more details. Uses various codes to describe authentication.

Table 57 - Mental Models Summary

PARTICIPANT	MENTAL MODELS SUMMARY
P01	Often separates the operating system from the physical device. Accounts for the operating system transferring information to apps as well as separate processes for authentication represented as a key icon that unlocks personal information.
P02	Many primary app preceded the tertiary app in the mental models.

P03	Has clear interaction paths. Reuses several magnetic icons to depict different sites of interaction especially during tertiary and secondary authentication.
P04	Verbal thinker. Thinks with words and less with icons. She signifies entering a password with the email icon because she it is part of her user account handle when performing verifications during authentication. Does not use modalities. Rarely uses devices as site of interaction.
P05	In some of her models, the primary app was presented before the secondary or tertiary app. Most of the models are abstract. By putting the primary app first, she signifies that she interact with that platform first and then jumps into the secondary or tertiary one.
P06	Does not use modalities. Does not depict devices. Mentions log but may not depict initial authentication. Abstract models.
P07	The mental models are mostly abstract but show an awareness of authentication both for login and logouts.
P08	Uses simple and abstract models that do not always depict authentication but mix modalities in the interaction path or outside of it in parallel with actions.
P09	The modalities are mixed within the interaction path. The model is linear without the use of paired icons. The initial site of interaction is clear.
P10	Depicts choices for authentication and paths not pursued instead of ignoring them. This is an attempt to depict reality as opposed to just her own interaction. Does not use the modalities.
P11	For the participant, the las site of interaction matters. Even a login using a modality is seen as a break with the previous site of interaction, even if the participant has not left the platform. The models are abstract and simple Modalities are within the path of interaction.
P12	Uses modalities as adjunct that are outside of the path to interaction yet connect from the initial site of interaction if it is the laptop. Rare mention of authentication although any processes were denied by the participant.
P13	Use of modalities as action within the path of interaction. The primary apps involved in the tertiary authentication are depicted as outside of the path of interaction.
P14	Very abstract models that use mathematical metaphors but also includes modalities. A focus on task completion. Authentication addressed and observed but not a central focus.
P15	Everything is on the interaction path but may have a floating label. The device and the app are the start of the site of interaction. There are side paths created. Logout is often depicted. Changing mental models with several errors and complex diagramming.
P16	Mixes abstract and physical models starting with devices such as the laptop. Groups the account icon with Facebook when representing authentication. Uses few modalities. Authentication is on the interaction path. Uses paired icons. Learning effect and changes in the mental models can be observed as she started using paired icons for tablets and their operating systems, and authentication. Uses less modalities over time.
P17	Is very literal with mental models. Describes every step as a site of interaction, as well as every action closely. Relies mostly on physical models. Explains authentication clearly. Does not use interaction modalities.

P18	Mental models are not linear and mostly abstract. Sometimes only uses magnetic icons as logos and not sites of interaction. Mental models rarely represent physical devices and are imaginative, not interaction-based.
P19	Uses the Internet magnetic icon to represent something being exchanged or accesses before authentication. Mixes physical models (laptop, mouse, and keyboard) with abstract models (Internet magnetic icon). Many connections and nodes between physical devices who stand outside of the interaction path but are used at many points.
P20	Uses abstract models to represent feedback arrows between primary and tertiary systems. Groups devices together in the feedback path between apps. Uses physical models to represent devices which are part of the interaction. Tends to represent interaction as linear outside of the feedback directional arrows.

Table 58 - Is there a login?

IS THERE A LOGIN?

	T3A		
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	6	30.0
	Yes	14	70.0
	Total	20	100.0
	T4B		
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	1	5.0
	Yes	19	95.0
	Total	20	100.0
	T5C		
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	9	45.0
	Yes	11	55.0
	Total	20	100.0
	T8A		
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	1	5.0
	Yes	19	95.0
	Total	20	100.0
	T9B		
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	3	15.0
	Yes	17	85.0
	Total	20	100.0
	T10C		
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	2	10.0
	Yes	18	90.0
	Total	20	100.0
	T13A		
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	3	15.0
	Yes	17	85.0
	Total	20	100.0
	T14B		
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	Yes	20	100.0
	T15C		

		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	3	15.0
	Yes	17	85.0
	Total	20	100.0

Table 59 - Is there a logout?

IS THERE A LOGOUT (PC) OR AN EXIT FROM THE APP (MOBILE)?

		Frequency	Percent
T3A			
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
T4B			
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
T5C			
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	14	70.0
	Yes	6	30.0
	Total	20	100.0
T8A			
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	13	65.0
	Yes	7	35.0
	Total	20	100.0
T9B			
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	13	65.0
	Yes	7	35.0
	Total	20	100.0
T10C			
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
T13A			
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	15	75.0
	Yes	5	25.0
	Total	20	100.0
T14B			
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	No	14	70.0
	Yes	6	30.0
	Total	20	100.0
T15C			
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	14	70.0
	Yes	6	30.0
	Total	20	100.0

Table 60 - Modalities of Interaction

ARE THERE MODALITIES OF INTERACTIONS?

		T3A	
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	10	50.0
	Yes	10	50.0
	Total	20	100.0
		T4B	
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	11	55.0
	Yes	9	45.0
	Total	20	100.0
		T5C	
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
		T8A	
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	17	85.0
	Yes	3	15.0
	Total	20	100.0
		T9B	
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	10	50.0
	Yes	10	50.0
	Total	20	100.0
		T10C	
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	10	50.0
	Yes	10	50.0
	Total	20	100.0
		T13A	
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
		T14B	
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	No	10	50.0
	Yes	10	50.0
	Total	20	100.0
		T15C	
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	15	75.0
	Yes	5	25.0
	Total	20	100.0

Table 61 - Modalities of interaction on path

ARE THE MODALITIES ON THE INTERACTION PATH?

T3A			
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	13	65.0
	Yes	7	35.0
	Total	20	100.0
T4B			
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	13	65.0
	Yes	7	35.0
	Total	20	100.0
T5C			
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
T8A			
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	17	85.0
	Yes	3	15.0
	Total	20	100.0
T9B			
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
T10C			
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	15	75.0
	Yes	5	25.0
	Total	20	100.0
T13A			
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	13	65.0
	Yes	7	35.0
	Total	20	100.0
T14B			
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
T15C			
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	16	80.0
	Yes	4	20.0
	Total	20	100.0

Table 62 - Primary / tertiary relationship

RELATIONSHIPS BETWEEN PRIMARY AND TERTIARY INDICATED?

T3A			
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	10	50.0
	Yes	10	50.0
	Total	20	100.0
T4B			
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	1	5.0
	Yes	19	95.0
	Total	20	100.0
T5C			
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	18	90.0
	Yes	2	10.0
	Total	20	100.0
T8A			
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	4	20.0
	Yes	16	80.0
	Total	20	100.0
T9B			
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	4	20.0
	Yes	16	80.0
	Total	20	100.0
T10C			
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	4	20.0
	Yes	16	80.0
	Total	20	100.0
T13A			
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	3	15.0
	Yes	17	85.0
	Total	20	100.0
T14B			
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	Yes	20	100.0
T15C			
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	8	40.0
	Yes	12	60.0
	Total	20	100.0

Table 63 - Reaction to access rights

REACTION TO REQUESTED ACCESS RIGHTS?

T3A			
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
T4B			
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	6	30.0
	Yes	14	70.0
	Total	20	100.0
T5C			
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	18	90.0
	Yes	2	10.0
	Total	20	100.0
T8A			
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	7	35.0
	Yes	13	65.0
	Total	20	100.0
T9B			
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	12	60.0
	Yes	8	40.0
	Total	20	100.0
T10C			
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	15	75.0
	Yes	5	25.0
	Total	20	100.0
T13A			
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	10	50.0
	Yes	10	50.0
	Total	20	100.0
T14B			
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	No	9	45.0
	Yes	11	55.0
	Total	20	100.0
T15C			
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	16	80.0
	Yes	4	20.0
	Total	20	100.0

Table 64 - Linear path

IS THE PATH LINEAR?

		T3A	
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	1	5.0
	Yes	19	95.0
	Total	20	100.0
		T4B	
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	1	5.0
	Yes	19	95.0
	Total	20	100.0
		T5C	
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	Yes	20	100.0
		T8A	
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	3	15.0
	Yes	17	85.0
	Total	20	100.0
		T9B	
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	3	15.0
	Yes	17	85.0
	Total	20	100.0
		T10C	
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	4	20.0
	Yes	16	80.0
	Total	20	100.0
		T13A	
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	2	10.0
	Yes	18	90.0
	Total	20	100.0
		T14B	
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	Yes	20	100.0
		T15C	
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	3	15.0
	Yes	17	85.0
	Total	20	100.0

Table 65 - Model

IS THE MODEL ABSTRACT OR PHYSICAL?

T3A			
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	Abstract	5	25.0
	Physical	15	75.0
	Total	20	100.0
T4B			
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	Abstract	7	35.0
	Physical	13	65.0
	Total	20	100.0
T5C			
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	Abstract	6	30.0
	Physical	14	70.0
	Total	20	100.0
T8A			
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	Abstract	5	25.0
	Physical	15	75.0
	Total	20	100.0
T9B			
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	Abstract	4	20.0
	Physical	16	80.0
	Total	20	100.0
T10C			
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	Abstract	7	35.0
	Physical	13	65.0
	Total	20	100.0
T13A			
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	Abstract	6	30.0
	Physical	14	70.0
	Total	20	100.0
T14B			
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	Abstract	5	25.0
	Physical	15	75.0
	Total	20	100.0
T15C			
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	Abstract	5	25.0
	Physical	15	75.0
	Total	20	100.0

Table 66 - Pairs

ARE THERE PAIRED MAGNETIC ICONS?

		T3A	
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	15	75.0
	Yes	5	25.0
	Total	20	100.0
		T4B	
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	15	75.0
	Yes	5	25.0
	Total	20	100.0
		T5C	
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	14	70.0
	Yes	6	30.0
	Total	20	100.0
		T8A	
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	13	65.0
	Yes	7	35.0
	Total	20	100.0
		T9B	
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	13	65.0
	Yes	7	35.0
	Total	20	100.0
		T10C	
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	17	85.0
	Yes	3	15.0
	Total	20	100.0
		T13A	
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	16	80.0
	Yes	4	20.0
	Total	20	100.0
		T14B	
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	No	16	80.0
	Yes	4	20.0
	Total	20	100.0
		T15C	
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	16	80.0
	Yes	4	20.0
	Total	20	100.0

Table 67 - Preceding primary

DOES THE PRIMARY PLATFORM PRECEDE THE TERTIARY AUTHENTICATION?

T3A			
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	3	15.0
	Yes	17	85.0
	Total	20	100.0
T4B			
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	17	85.0
	Yes	3	15.0
	Total	20	100.0
T5C			
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	2	10.0
	Yes	18	90.0
	Total	20	100.0
T8A			
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	18	90.0
	Yes	2	10.0
	Total	20	100.0
T9B			
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	20	100.0
T10C			
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	16	80.0
	Yes	4	20.0
	Total	20	100.0
T13A			
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	19	95.0
	Yes	1	5.0
	Total	20	100.0
T14B			
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	No	13	65.0
	Yes	7	35.0
	Total	20	100.0
T15C			
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	11	55.0
	Yes	9	45.0
	Total	20	100.0

Table 68 - Tertiary authentication and path

IS THE TERTIARY AUTHENTICATION PART OF THE INTERACTION PATH?

T3A			
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	3	15.0
	Yes	17	85.0
	Total	20	100.0
T4B			
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	4	20.0
	Yes	16	80.0
	Total	20	100.0
T5C			
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	19	95.0
	Yes	1	5.0
	Total	20	100.0
T8A			
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	5	25.0
	Yes	15	75.0
	Total	20	100.0
T9B			
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	6	30.0
	Yes	14	70.0
	Total	20	100.0
T10C			
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	7	35.0
	Yes	13	65.0
	Total	20	100.0
T13A			
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	5	25.0
	Yes	15	75.0
	Total	20	100.0
T14B			
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	No	4	20.0
	Yes	16	80.0
	Total	20	100.0
T15C			
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	6	30.0
	Yes	14	70.0
	Total	20	100.0

Table 69 - Differentiation

DIFFERENTIATION OF THE OPERATING SYSTEM FROM THE DEVICE (MOBILE), THE BROWSER FROM THE PC (PC), OR INDICATION OF AN INDEPENDENT INTERNET (BOTH).

		T3A	
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	No	8	40.0
	Yes	12	60.0
	Total	20	100.0
		T4B	
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	No	9	45.0
	Yes	11	55.0
	Total	20	100.0
		T5C	
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	No	10	50.0
	Yes	10	50.0
	Total	20	100.0
		T8A	
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	No	14	70.0
	Yes	6	30.0
	Total	20	100.0
		T9B	
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	No	16	80.0
	Yes	4	20.0
	Total	20	100.0
		T10C	
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	No	10	50.0
	Yes	10	50.0
	Total	20	100.0
		T13A	
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	No	14	70.0
	Yes	6	30.0
	Total	20	100.0
		T14B	
		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	No	5	25.0
	Yes	15	75.0
	Total	20	100.0
		T15C	
		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	No	16	80.0
	Yes	4	20.0
	Total	20	100.0

Table 70 - Initial site of interaction

WHERE IS THE INITIAL SITE OF INTERACTION?

		T3A	
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	AngryBirds	1	5.0
	AngryBirds and Facebook	1	5.0
	Facebook	3	15.0
	Laptop	14	70.0
	Laptop and Firefox	1	5.0
	Total	20	100.0
		T4B	
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	dlvr.it	5	25.0
	Facebook	1	5.0
	Laptop	12	60.0
	Laptop, Firefox, and dlvr.it	1	5.0
	Laptop, Internet, and mouse	1	5.0
	Total	20	100.0
		T5C	
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	BlackBerry	6	30.0
	BlackBerry and tablet	7	35.0
	Facebook	3	15.0
	Tablet	4	20.0
	Total	20	100.0
		T8A	
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	Hootsuite	4	20.0
	Internet and iPad	1	5.0
	iPad	5	25.0
	iPad, tablet, iOS	1	5.0
	Tablet	6	30.0
	Tablet and Hootsuite	1	5.0
	Tablet and iOS	2	10.0
	Total	20	100.0
		T9B	
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	Android	1	5.0
	Tablet	12	60.0
	Tablet and Android	2	10.0
	Tablet and Talon	2	10.0
	Talon	2	10.0
	Vine	1	5.0
	Total	20	100.0
		T10C	
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	Laptop	12	60.0
	Medium	5	25.0

	Person	1	5.0
	Twitter	1	5.0
	Twitter and Medium	1	5.0
	Total	20	100.0

T13A

		Frequency	Percent
TASK 13 - SPARK **TERTIARY CLIENT APP CLONE**	Google	1	5.0
	iPad	3	15.0
	Spark	4	20.0
	Tablet	9	45.0
	Tablet and iOS	2	10.0
	Tablet and Spark	1	5.0
	Total	20	100.0

T14B

		Frequency	Percent
TASK 14 - DROPBOX **TERTIARY SERVICE & PRODUCT APP**	Dropbox	1	5.0
	Firefox	2	10.0
	Google	3	15.0
	Laptop	13	65.0
	Laptop, Firefox, and Dropbox	1	5.0
	Total	20	100.0

T15C

		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS **TERTIARY DATA MANIPULATION APP**	Android	1	5.0
	Android and tablet	1	5.0
	Business Organizer	1	5.0
	Business Organizer and Docs	1	5.0
	Google	3	15.0
	iPad	1	5.0
	Tablet	11	55.0
	Tablet and Business Organizer	1	5.0
	Total	20	100.0

Table 71 - Last site of interaction

WHERE IS THE LAST SITE OF INTERACTION?

		T3A	
		Frequency	Percent
TASK 3 - ANGRYBIRDS FRIENDS TERTIARY SERVICE & PRODUCT APP	AngryBirds	15	75.0
	Facebook	2	10.0
	Firefox	3	15.0
	Total	20	100.0
		T4B	
		Frequency	Percent
TASK 4 - DLVR.IT TERTIARY DATA MANIPULATION APP	ComicBookBin	1	5.0
	dlvr.it	14	70.0
	dlvr.it, Facebook	1	5.0
	Facebook	1	5.0
	Firefox	2	10.0
	RSS	1	5.0
	Total	20	100.0
		T5C	
		Frequency	Percent
TASK 5 - PLAYBOOK FACEBOOK CLONE (BLACKBERRY) TERTIARY CLIENT APP CLONE	Facebook	20	100.0
		T8A	
		Frequency	Percent
TASK 8 - HOOTSUITE TERTIARY DATA MANIPULATION APP	Google	1	5.0
	Hootsuite	5	25.0
	iPad	3	15.0
	Twitter	10	50.0
	Twitter and Hootsuite	1	5.0
	Total	20	100.0
		T9B	
		Frequency	Percent
TASK 9 - TALON TERTIARY CLIENT APP CLONE	New Yorker article	1	5.0
	Tablet	1	5.0
	Talon	8	40.0
	Talon and Twitter	1	5.0
	Twitter	9	45.0
	Total	20	100.0
		T10C	
		Frequency	Percent
TASK 10 - MEDIUM TERTIARY SERVICE & PRODUCT APP	Firefox	2	10.0
	Medium	15	75.0
	Person	1	5.0
	Twitter	1	5.0
	Twitter and Medium	1	5.0
	Total	20	100.0
		T13A	
		Frequency	Percent
TASK 13 - SPARK TERTIARY CLIENT APP CLONE	dlvr.it	1	5.0
	Email to person	3	15.0
	Gmail	1	5.0
	Google	4	20.0
	iPad	2	10.0
	Spark	7	35.0
	Tablet	2	10.0
	Total	20	100.0
		T14B	

		Frequency	Percent
TASK 14 - DROPBOX TERTIARY SERVICE & PRODUCT APP	Dropbox	12	60.0
	Email	1	5.0
	Firefox	4	20.0
	Google	3	15.0
	Total	20	100.0

T15C

		Frequency	Percent
TASK 15 - BUSINESS ORGANIZER FOR GOOGLE DOCS TERTIARY DATA MANIPULATION APP	Business Organizer	7	35.0
	Business Organizer and Docs	1	5.0
	Docs	8	40.0
	Google	2	10.0
	Loop	2	10.0
	Total	20	100.0

Table 72- First Pass Qualitative Coding

QUESTION	**12-DID YOU NOTICE ANY DIFFERENCES BETWEEN THE DIFFERENT WAYS THAT YOU LOGGED INTO EACH PLATFORM AND APP? EXPLAIN IN YOUR OWN WORDS.**			
Q12	Coder 1	Count	Coder 2	Count
	Not many differences	1	Did not notice differences	3
	Yes	4	Few differences (or superficial only)	1
	No	3	Some differences	14
	Use same language to explain That I use Facebook, Google, Twitter	1	Comment related to difficulty/ease of use / "streamlined"	8
	Some processes are more complicated than others	2	Comment related to what info was shared	3
	Some more streamlined	2	Comment related to visual differences	2
	2 step authentication problems	1	Described process but no normative judgment	1
	Laptop easier	3		
	iPad easy	1		
	Tablets more difficult	2		
	Tablets easy	1		
	Visual cues/options different	3		
	Lack of rationale for tertiary authentication	2		

	Usable (convenient, streamlined)	1		
	Explains choice presented by apps	1		
	Explains personal choices	1		
	Unable to log into tertiary apps	1		
	Additional options, information requested	1		
QUESTION	13-Did you experience any difficulty while logging into the different platforms and apps? Explain in your own words.			
Q13	Coder 1	Count	Coder 2	Count
	No	7	No difficulty	5
	sometimes	1	Minimal difficulty	3
	Yes	10	Yes difficulty	7
	Spark problems	1	Remembering log information (username & passwords)	4
	Dislike typing long email addresses	1	Error messages or crashes	2
	Forgot password	4	Difficulty with specific software	5
	Two-factor authentication problems	1		
	I know my account well (literacy)	1		
	Too many screens/pop ups	1		
	BlackBerry Playbook problems	2		
	Error messages	1		
	Wi-Fi problems	1		
	Hootsuite conflict between Google and Twitter	1		
QUESTION	14- How did you feel about logging into Facebook, Google, and Twitter to perform tasks? Did you have any concerns about the security of your information?			
Q14	Coder 1	Count	Coder 2	Count
	No	7	No concern	7

	Felt secure	1	Yes concern	10
	Yes	5	Self-management of private/public information	5
	Somewhat/slightly	4	Perceived lack of control about how & what information is circulated	4
	Safety because of study	2	Reassured by this study context	2
	Had concerns	2		
	Convenient	1		
	Uses it regardless of concerns	1		
	Keep personal info off	1		
	Apps posting to page without consent	1		
	Dislikes creating new password after tertiary authentication	1		
	Password challenging to enter on tablets	1		
QUESTION	15- What security measures would you take to secure yourself when you log in to Facebook, Google, and/or Twitter?			
Q15	Coder 1	Count	Coder 2	Count
	Review tertiary apps access	1	Change passwords	3
	Mindful of place of interaction (in public)	3	Strong passwords / two-factor	3
	Change passwords regularly	3	Wary of public computers, public places etc. (or other security flaws in hardware endpoint	4
	Adjust privacy/security settings	3	Privacy settings and security settings	5
	Use a private browser mode	1	Limit what they post	3
	Limit usage/postings	3	Wary of third party apps	3
	Strong passwords	3		
	Use password manager	1		
	Do nothing	1		
	Limit information seeking	2		

	Two-factor authentication	1		
	Use known devices	2		
	Trustworthy/recommended	1		
	No information shared in public	1		
	Do not share authentication key	1		
QUESTION	16-What are some of the tips that you would give an acquaintance to remain secure when using Facebook, Google, and/or Twitter?			
Q16	Coder 1	Count	Coder 2	Count
	Use separate passwords	1	Change passwords	3
	Multifactor authentication	2	Strong passwords / two-factor	7
	Complicated passwords	1	Wary of public computers, public places etc.	3
	Adjust settings/options	4	Privacy settings and security settings	5
	Change passwords	3	Limit what they post	6
	Use private settings	2	Wary of third party apps	1
	Always log out	1		
	Be careful of posts' contents	4		
	Delete cookies and cache	1		
	RoboForm	1		
	Be mindful of place of interaction	3		
	Uniform identity	1		
	Multiple identity	1		
	Do not use	1		
	Trusted source	1		
	Limit 3rd party access to platform	1		
	Higher security level	1		
QUESTION	17-Do you feel that your information is safer because Instagram, Google Docs, and Vine are owned respectively by Facebook, Google, and Twitter?			

Q17	Coder 1	Count	Coder 2	Count
	Somewhat/maybe	4	No	7
	Affirmative (yes)	6	Somewhat	5
	Neutral	1	Yes	8
	Negative	7		
	Unaware	1		

QUESTION	Coder 1	Count	Coder 2	Count
Q18				

18-WHAT HAPPENS TO YOUR INFORMATION FROM INSTAGRAM, GOOGLE DOCS, AND VINE IF YOU DELETE YOUR FACEBOOK, GOOGLE, AND, OR TWITTER ACCOUNTS?

	Does not know	7	Deleted	4
	Believe/would like it deleted	6	Varies by platform	1
	Is kept	9	Not deleted	8
	Kept temporarily	1	Confident	6
			Unsure	9

QUESTION	Coder 1	Count	Coder 2	Count
Q19				

19-IF YOU DELETE YOUR FACEBOOK, GOOGLE, AND/OR TWITTER ACCOUNT, WHAT SHOULD HAPPEN WITH THE INFORMATION COLLECTED INDEPENDENTLY BY DLVR.IT, ORGANIZER FOR GOOGLE, SPARK, HOOTSUITE, FACEBOOK FOR BLACKBERRY PLAYBOOK, TALON, DROPBOX, ANGRYBIRDS FRIENDS, AND/OR MEDIUM?

	Should be deleted	11	Should be deleted (or option to delete it	12
	Doesn't know	2	Would be kept (seems like they answered what *will * happen instead of what *should* happen)	6
	Information stays	3	Don't know	2
	Option to delete at account termination	3		
	Information stays but no option to delete	1		

QUESTION	Coder 1	Count	Coder 2	Count2
Q20				
20-IN YOUR WORDS, WHAT ARE SECURITY AND CONFIDENTIALITY? ARE THEY THE SAME? WHAT ABOUT PRIVACY?				
	Security = data protection	11	Confidentiality and privacy are the same (or similar)	3
	Security = passwords	1	Don't know difference (or how to define one of the terms)	2
	I don't know	2	Security - prevent intruders or unauthorized use	6
	Security, confidentiality not the same	3	Privacy is about being able to control personal information	5
	Security = prevent access	1	Privacy is about keeping personal info from others	4
	Security = level of trust	1	Security is about keeping personal info from others	7
	Security = piece of mind	1	Control, self-determination	5
	Confidentiality = about party sharing your information	7	Expresses ownership of data ("my data" "my space" "your property")	8
	Confidentiality related to privacy	4		
	Security = confidentiality	1		
	Privacy = apps should not monitor activity	1		
	Confidentiality = choosing with whom can be shared	2		
	Security = authentication, authorization	1		
	Security = someone I don't know can access my information	2		
	Security & confidentiality = how information is kept	1		
	Confidentiality = sensitivity to personal information	1		
	Confidentiality = keep private information safe	1		
	Confidentiality = anonymous information	1		

	Confidentiality = stored with you or elsewhere	1
	Privacy is a principle	2
	Privacy = information withheld from public	2
	Privacy = information not encroached on	1
	Privacy = who should have access to information	2
	Privacy = keeping information to oneself	4

Table 73 - Open Questions Second Pass Coding

Open Questions Second Pass Coding

Q12

		Frequency	Percent
Did you notice any differences between the different ways that you logged into each platform and app? Explain in your own words.	No	3	15.0
	Yes	13	65.0
	Neutral with explanation	4	20.0
	Total	20	100.0

Q13

		Frequency	Percent
Did you experience any difficulty while logging into the different platforms and apps? Explain in your own words.	Yes	12	60.0
	No	8	40.0
	Total	20	100.0

Q14

		Frequency	Percent
How did you feel about logging into Facebook, Google, and Twitter to perform tasks? Did you have any concerns about the security of your information?	Yes	10	50.0
	No	8	40.0
	Neutral with explanation	2	10.0
	Total	20	100.0

Q15

		Frequency	Percent
What security measures would you take to secure yourself when you log in to Facebook, Google, and/or Twitter?	Change passwords	2	10.0
	Strong passwords	2	10.0
	Control over place of Interaction	2	10.0
	Limit postings	4	20.0
	Privacy and Security settings	4	20.0
	Control used devices and apps	4	20.0
	Change passwords; Privacy and Security settings; Control over place of Interaction	1	5.0
	None	1	5.0
	Total	20	100.0

Q16

		Frequency	Percent
What are some of the tips that you would give an acquaintance to remain secure when using Facebook, Google, and/or Twitter?	Change passwords	1	5.0
	Private and security settings	6	30.0
	Multifactor and strong passwords	4	20.0
	Control over what is posted	6	30.0
	Private and security settings; Change passwords	1	5.0
	Private and security settings; Multifactor and strong passwords	1	5.0
	Change passwords; Control over place of Interaction	1	5.0
	Total	20	100.0

Q17

		Frequency	Percent
Do you feel that your information is safer because Instagram, Google Docs, and Vine are owned respectively by Facebook, Google, and Twitter?	Yes	12	60.0
	No	7	35.0
	Neutral with explanation	1	5.0
	Total	20	100.0

Q18

		Frequency	Percent
What happens to your information from Instagram, Google Docs, and Vine if you delete your Facebook, Google, and, or Twitter accounts?	Is kept	8	40.0
	Deleted	5	25.0
	Unsure	7	35.0
	Total	20	100.0

Q19

		Frequency	Percent
If you delete your Facebook, Google, and/or Twitter account, what should happen with the information collected independently by dlvr.it, Organizer for Google, Spark, Hootsuite, Facebook for BlackBerry Playbook, Talon, Dropbox, AngryBirds Friends, and/or Medium?	Should be deleted	13	65.0
	Information stays	5	25.0
	Don't know	2	10.0
	Total	20	100.0

Q20

		Frequency	Percent
In your words, what are security and confidentiality? Are they the same? What about privacy?	Security is related to confidentiality	1	5.0
	Security is not related to confidentiality	16	80.0
	Security and confidentiality, unsure	3	15.0
	Total	20	100.0