

PRIVACY AWARENESS AND DESIGN FOR LIVE VIDEO BROADCASTING  
APPS

by

Dhuha Al-Amiri

Submitted in partial fulfilment of the requirements  
for the degree of Master of Computer Science

at

Dalhousie University  
Halifax, Nova Scotia  
August 2016

© Copyright by Dhuha Al-Amiri, 2016

# Dedication

I dedicate this thesis to:

*To my mother,*

*Who has been devoting her time to pray for me and wishing me success, progress and approach to the best. To whom took care of me since my childhood, struggled and overcame difficulties, and shaped a positive environment since grade school in order to provide comfort and create the best atmosphere to learn and excel.*

*To my father,*

*Who dedicated his life and struggled to give us a decent life. To the person who always supports and encourages me, and continuously feeds me with ambition and determination to surpass and be among the best.*

*I hope, with the work I've done, that I presented a lovely gift to my parents, and that it would make them proud of me forever, even if it was something so simple as opposed to what they have given me.*

*To my husband,*

*Who was like a mother and a father to me in my journey, who strived for my comfort and shared the difficult times that I went through, and was so encouraging to make me stand up and keep working. I wish I could make up for some of what he has given me.*

# TABLE OF CONTENTS

<b>LIST OF TABLES .....</b>	<b>vii</b>
<b>LIST OF FIGURES.....</b>	<b>xi</b>
<b>ABSTRACT .....</b>	<b>xiii</b>
<b>LIST OF ABBREVIATIONS USED .....</b>	<b>xiv</b>
<b>ACKNOWLEDGEMENTS .....</b>	<b>xv</b>
<b>CHAPTER 1 INTRODUCTION.....</b>	<b>1</b>
1.1 PRIVACY AND PRIVACY AWARENESS.....	2
1.2 OVERVIEW OF THESIS.....	4
1.3 THESIS STRUCTURE .....	5
<b>CHAPTER 2 LITERATURE REVIEW .....</b>	<b>6</b>
2.1 AN OVERVIEW OF SOCIAL MEDIA.....	7
2.1.1 <i>Use and Impacts of Social Media</i> .....	7
2.1.2 <i>The Emergence of Video in Social Media</i> .....	10
2.1.3 <i>Temporal Social Media (Live Video Broadcasting)</i> .....	14
2.2 PRIVACY AND SELF-DISCLOSURE OF INFORMATION .....	20
2.2.1 <i>Factors Influencing Privacy and Self-Disclosure</i> .....	21
2.2.2 <i>Privacy and Self-Disclosure in Social Media</i> .....	23
2.2.3 <i>Privacy Awareness Support</i> .....	26
2.3 PRIVACY ISSUES ASSOCIATED WITH LIVE VIDEO BROADCASTING.....	27
2.3.1 <i>Location Information</i> .....	28
2.3.2 <i>Visual Privacy Protection</i> .....	34
<b>CHAPTER 3 USE AND PRIVACY PERCEPTION EXPLORATION.....</b>	<b>38</b>
3.1 GENERAL APPROACH AND METHODS .....	38
3.1.1 <i>Participant Recruitment</i> .....	39
3.1.2 <i>Study Procedure</i> .....	39
3.1.3 <i>Research Questions</i> .....	40

3.1.4 Study Instrument and Measures.....	40
3.1.5 Analytic Plan and General Comments on Issues for Statistical Analyses.....	43
3.2 RESULTS .....	53
3.2.1 Participant Demographics.....	53
3.2.2 Data Cleaning .....	54
3.2.3 Apps Used.....	55
3.2.4 Reasons for Use .....	56
3.2.5 Categories of Use .....	59
3.2.6 Concerns and Issues .....	69
3.2.7 Periscope Use .....	80
3.2.8 Relationships between Variables .....	87
3.3 DISCUSSION.....	118
3.3.1 Participants Demographic.....	118
3.3.2 Live Video Apps Use.....	119
3.3.3 Categories of Broadcasts and Privacy.....	120
3.3.4 Broadcast Locations and Privacy Issues.....	120
3.3.5 Mood and Privacy .....	121
3.3.6 Privacy Concerns with Broadcasts .....	122
3.3.7 Knowledge about Temporal Live Video Broadcasting Apps .....	122
3.3.8 Pros and Cons of Temporary Nature Live Broadcasts.....	123
3.3.9 The Desire for Privacy on Live Video Broadcasts.....	124
3.3.10 The Privacy of Sensitive Information.....	124
3.3.11 Periscope Users and Privacy.....	125
3.4 LIMITATIONS AND FUTURE WORK.....	126
3.4.1 Validity.....	127
3.4.2 Reliability.....	127
<b>CHAPTER 4 DESIGN OF PRIVACY AWARENESS MECHANISMS.....</b>	<b>132</b>
4.1 LOCATION VIEWERS FEEDBACK PROTOTYPES (LVFPs) .....	132
4.1.1 Theoretical Foundation: .....	132
4.1.2 Design 1: GeoLocate (GL) Prototype.....	135

4.1.3 Design 2: GeoWatch (GW) Prototype.....	139
4.1.4 Design 3: GeoBar (GB) Prototype.....	143
4.2 VISUAL PRIVACY AWARENESS PROTOTYPES (VPAPS) .....	146
4.2.1 Theoretical Foundation: .....	146
4.2.2 Matching Mood-to-Mood Task (MMT) .....	149
4.2.3 Appearance-to-Mood Task (AMT).....	157
4.2.4 Choosing Your Appearance Directly Task (ADT).....	164
4.3 DESIGN EVALUATION PROCEDURE .....	169
4.3.1 Participants and recruitment.....	170
4.3.2 Study Procedure.....	170
4.3.3 Location Viewers Feedback Experiment.....	171
4.3.4 Visual Privacy Awareness Experiment.....	172
4.4 RESULTS .....	173
4.4.1 Participants Demographic.....	173
4.4.2 Self-Reported Behavior of Participants.....	174
4.4.3 Comparison of Prototypes.....	182
4.4.3.1 Location Viewers Feedback Prototypes (GeoLocate, GeoWatch, GeoBar).....	182
4.4.3.1.1 Feedback from Participants .....	204
4.4.3.1.2 Suggestions for Location Viewers Feedback Designs.....	209
4.4.3.2 Visual Privacy Awareness Prototypes (Mood-to-Mood, Appearance-to-Mood, Appearance-Directly).....	211
4.4.3.2.1 Feedback from Participants .....	215
4.4.3.2.2 Suggestions for the Visual Privacy Awareness Designs.....	217
4.5 DISCUSSION.....	218
4.5.1 Participants Demographic.....	218
4.5.2 Live Video Broadcasting Use.....	219
4.5.3 Comparison of Location Viewers Feedback Prototypes.....	219
4.5.3.1 Attention.....	219
4.5.3.2 Ease of Use/Ease of Finding Information.....	220
4.5.3.3 Understandability and Clarity.....	221
4.5.4 Design Implications for Location Viewers Feedback.....	224

4.5.5 Comparisons of Visual Privacy Awareness Prototypes.....	226
4.5.6 Design Implications for Visual privacy Awareness.....	227
4.6 LIMITATIONS.....	229
4.6.1 Location Viewers Feedback Experiment.....	229
4.6.2 Visual Privacy Awareness Experiment.....	230
4.7 FUTURE WORK.....	231
4.7.1 Location Viewers Feedback Prototypes.....	231
4.7.2 Visual Privacy Awareness Prototypes.....	232
<b>CHAPTER 5 CONCLUSION.....</b>	<b>234</b>
5.1 STUDY 1 AND STUDY 2.....	235
5.2 THESIS CONTRIBUTION.....	236
5.3 LIMITATIONS.....	237
5.4 FUTURE WORK.....	238
<b>BIBLIOGRAPHY.....</b>	<b>240</b>
<b>Appendix A – Recruitment Notice.....</b>	<b>254</b>
<b>Appendix B – Consent Form.....</b>	<b>255</b>
<b>Appendix C – Online Survey.....</b>	<b>257</b>
<b>Appendix D – Recruitment Notice.....</b>	<b>278</b>
<b>Appendix E – Consent Form.....</b>	<b>279</b>
<b>Appendix F – Background Information.....</b>	<b>281</b>
<b>Appendix G – Questionnaire for Location Viewers Feedback Prototypes.....</b>	<b>288</b>
<b>Appendix H – Questionnaire for Visual Privacy Awareness Prototypes.....</b>	<b>294</b>
<b>Appendix I – Participant Payment Receipt.....</b>	<b>299</b>

## LIST OF TABLES

TABLE 2.1	DIMENSIONS OF PRIVACY-AWARENESS INFORMATION.....	26
TABLE 3.1	USE OF APPS.....	55
TABLE 3.2	MEANS AND ANALYSIS OF GROUP DIFFERENCES FOR MAXIMUM INTENSITY OF USE.....	56
TABLE 3.3	REASONS FOR USING LIVE STREAMING VIDEO APPS. ....	57
TABLE 3.4	CORRELATIONS BETWEEN REASONS FOR USE. ....	58
TABLE 3.5	CATEGORIES OF BROADCASTS (BCs) AND THE TYPES OF AUDIENCE FOR EACH CATEGORY.....	60
TABLE 3.6	CORRELATIONS BETWEEN CATEGORIES OF BROADCASTS (BCs).....	61
TABLE 3.7	CATEGORIES OF BROADCASTS (BCs) AND THE ADJUSTED TYPES OF AUDIENCE FOR EACH CATEGORY .....	62
TABLE 3.8	CATEGORIES OF BROADCASTS (BCs) AND THE TYPES OF PLANNING FOR EACH CATEGORY.....	63
TABLE 3.9	CATEGORIES OF BROADCASTS (BCs) AND THE LOCATIONS OF THOSE BROADCASTS. ....	64
TABLE 3.10	CORRELATIONS BETWEEN THE LOCATIONS OF BROADCASTS.....	65
TABLE 3.11	CATEGORIES OF BROADCASTS (BCs) AND MOOD WHILE BROADCASTING. ....	66
TABLE 3.12	GENERAL MOOD WHILE BROADCASTING. ....	67
TABLE 3.13	CORRELATIONS BETWEEN MOODS WHILE BROADCASTING. ....	68
TABLE 3.14	RESTRICTIONS ON USE.....	69
TABLE 3.15	CONCERNS (OUT OF 3).....	70
TABLE 3.16	CORRELATIONS BETWEEN CONCERNS.....	71
TABLE 3.17	ENDORSEMENT OF POSITIVE FEATURES OF EPHEMERAL NATURE OF BROADCAST .....	72
TABLE 3.18	CORRELATIONS BETWEEN POSITIVE FEATURES OF THE EPHEMERAL NATURE OF BROADCASTS.....	73
TABLE 3.19	ENDORSEMENT OF NEGATIVE FEATURES FOR EPHEMERAL NATURE OF BROADCAST.....	74
TABLE 3.20	CORRELATIONS BETWEEN NEGATIVE FEATURES OF THE EPHEMERAL NATURE OF BROADCASTS.....	74
TABLE 3.21	ENDORSEMENT OF FEEDBACK OPTIONS .....	75
TABLE 3.22	CORRELATIONS BETWEEN FEEDBACK ITEMS .....	76

TABLE 3.23	ENDORSEMENT OF OPTIONS ABOUT INFORMATION THAT IS SENSITIVE (TO BE KEPT PRIVATE).....	77
TABLE 3.24	CORRELATIONS BETWEEN INFORMATION THAT IS SENSITIVE (TO BE KEPT PRIVATE) ...	77
TABLE 3.25	ENDORSEMENT OF OPTIONS CITING REASONS TO HIDE FACE OR VOICE.....	78
TABLE 3.26	CORRELATIONS BETWEEN REASONS TO HIDE FACE AND VOICE.....	79
TABLE 3.27	ENDORSEMENT OF OPTIONS CITING REASONS TO HIDE LOCATION (GPS).....	80
TABLE 3.28	CORRELATIONS BETWEEN REASONS TO HIDE LOCATION.....	80
TABLE 3.29	AUDIENCE CHOICE FOR PERISCOPE USERS.....	81
TABLE 3.30	RETENTION INTERVAL FOR BROADCASTS.....	83
TABLE 3.31	REASONS TO KEEP A VIDEO.....	83
TABLE 3.32	REASONS TO DELETE A VIDEO.....	84
TABLE 3.33	REVEALING LOCATION.....	85
TABLE 3.34	BENEFITS FOR REVEALING LOCATION.....	86
TABLE 3.35	RISKS FOR REVEALING LOCATION.....	86
TABLE 3.36	CORRELATION BETWEEN DEMOGRAPHIC MEASURES.....	88
TABLE 3.37	MEANS AND ANALYSIS OF GROUP DIFFERENCES FOR SEX, AGE, EDUCATION, COMFORT WITH TECHNOLOGY, KNOWLEDGE OF SECURITY.....	90
TABLE 3.38	PERCENT ENDORSEMENT BY GROUP (APPGRP) FOR REASONS FOR USE.....	91
TABLE 3.39	CATEGORY OF USE BY APPGRP.....	92
TABLE 3.40	PERCENTAGE OF RESPONDENTS ENDORSING EACH LEVEL OF AUDIENCE TYPE BY APPGRP.....	93
TABLE 3.41	PERCENTAGE OF RESPONDENTS ENDORSING EACH LEVEL OF PLANNING BY APPGRP.....	94
TABLE 3.42	LOCATION BY APPGRP.....	95
TABLE 3.43	MOOD BY APPGRP.....	96
TABLE 3.44	RESTRICTIONS BY APPGRP.....	97
TABLE 3.45	PERCENTAGE OF RESPONDENTS ENDORSING EACH LEVEL OF KNOWLEDGE ABOUT SAVING BY APPGRP.....	97
TABLE 3.46	PERCENTAGE OF RESPONDENTS ENDORSING EACH LEVEL OF KNOWLEDGE ABOUT RE-BROADCASTING BY APPGRP.....	98
TABLE 3.47	PERCENTAGE OF RESPONDENTS ENDORSING EACH LEVEL OF KNOWLEDGE ABOUT SAVING AND ABOUT RE-BROADCASTING.....	98
TABLE 3.48	RATINGS OF CONCERNS BY APPGRP.....	99



TABLE 3.49	PERCENTAGE OF RESPONDENTS ENDORSING THE GOOD AND BAD FEATURES OF THE TEMPORARY NATURE OF BROADCAST, BY APPGRP. ....	101
TABLE 3.50	REASONS FOR USE AND TYPES OF CONCERNS. ....	103
TABLE 3.51	REASONS FOR USE AND POSITIVE FEATURES OF THE TEMPORARY NATURE. ....	105
TABLE 3.52	REASONS FOR USE AND NEGATIVE FEATURES OF THE TEMPORARY NATURE. ....	107
TABLE 3.53	REASONS FOR USE AND INFORMATION THAT IS SENSITIVE (TO BE KEPT PRIVATE) .....	108
TABLE 3.54	REASONS FOR USE AND REASONS TO HIDE FACE. ....	110
TABLE 3.55	REASONS FOR USE AND REASONS TO HIDE VOICE. ....	111
TABLE 3.56	REASONS FOR USE AND REASONS TO HIDE LOCATION. ....	112
TABLE 3.57	MOOD AND REASONS TO HIDE FACE. ....	113
TABLE 3.58	PERISCOPE USERS: KNOWLEDGE OF LOCATION FEATURE AND THE LOCATION OF BROADCASTS .....	114
TABLE 3.59	PERISCOPE USERS: KNOWLEDGE OF LOCATION FEATURE AND THE LOCATION OF BROADCASTS .....	115
TABLE 3.60	PERISCOPE USERS: LOCATION AND RETENTION INTERVALS .....	116
TABLE 3.61	PERISCOPE USERS: AUDIENCE AND REASONS TO KEEP VIDEO .....	117
TABLE 3.62	PERISCOPE USERS: PERCENT ENDORSEMENT FOR AUDIENCE AND REASONS TO DELETE VIDRO .....	118
TABLE 4.1	USE OF APPS.....	174
TABLE 4.2	REASONS FOR USING LIVE STREAMING VIDEO APPS. ....	175
TABLE 4.3	CATEGORIES OF BROADCASTS AND THE TYPES OF AUDIENCE FOR EACH CATEGORY. ....	176
TABLE 4.4	CORRELATIONS BETWEEN CATEGORIES OF BROADCASTS (BCs).....	177
TABLE 4.5	CATEGORIES OF BROADCASTS (BCs) AND THE TYPES OF PLANNING FOR EACH CATEGORY.....	178
TABLE 4.6	CATEGORIES OF BROADCASTS (BCs) AND THE LOCATIONS OF THOSE BROADCASTS. ....	179
TABLE 4.7	CORRELATIONS BETWEEN THE LOCATIONS OF BROADCASTS.....	180
TABLE 4.8	ENDORSEMENT OF OPTIONS ABOUT SENSITIVE INFORMATION (TO BE KEPT PRIVATE) .....	180
TABLE 4.9	ENDORSEMENT OF OPTIONS ABOUT MOODS.....	182
TABLE 4.10	NUMBER OF VIEWERS IDENTIFIED CORRECTLY (OUT OF 8).....	182
TABLE 4.11	NUMBER OF PARTICIPANTS WHO CORRECTLY IDENTIFIED (CITED) THE INDIVIDUAL VIEWERS (OUT OF 8).....	184

TABLE 4.12	NUMBER OF PARTICIPANTS WHO CORRECTLY IDENTIFIED THE DISTANCE TO EACH (CITED) VIEWER (OUT OF 8).....	186
TABLE 4.13	NUMBER OF PARTICIPANTS WHO CORRECTLY IDENTIFIED THE INDIVIDUAL VIEWERS WHO SUDDENLY APPEARED ONSCREEN (OUT OF 2) .....	187
TABLE 4.14	NUMBER OF PARTICIPANTS WHO CORRECTLY IDENTIFIED THE INDIVIDUAL VIEWERS WHO SUDDENLY DISAPPEARED ONSCREEN (OUT OF 2) .....	189
TABLE 4.15	NUMBER OF PARTICIPANTS WHO CORRECTLY IDENTIFIED THE CLOSEST VIEWER.....	191
TABLE 4.16	NUMBER OF PARTICIPANTS WHO CORRECTLY IDENTIFIED THE FURTHEST VIEWER.....	192
TABLE 4.17	NUMBER OF PARTICIPANTS WHO CORRECTLY IDENTIFIED THE VIEWERS MOVING TOWARD THE BROADCASTER.....	193
TABLE 4.18	NUMBER OF PARTICIPANTS WHO CORRECTLY IDENTIFIED THE VIEWERS MOVING AWAY FROM THE BROADCASTER.....	194
TABLE 4.19	NUMBER OF PARTICIPANTS WHO CORRECTLY IDENTIFIED THE VIEWERS MOVING TOWARDS, THEN AWAY FROM THE BROADCASTER.....	196
TABLE 4.20	PERFORMANCE RANKING OF PROTOTYPES ACROSS TASKS .....	198
TABLE 4.21	QUESTION LIST FOR RATING PROTOTYPES.....	199
TABLE 4.22	ANALYSIS OF RATINGS AS A FUNCTION OF PROTOTYPES.....	201
TABLE 4.23	RANKINGS OF PROTOTYPES.....	202
TABLE 4.24	WHICH FEATURES ARE IMPORTANT? .....	203
TABLE 4.25	CORRELATIONS BETWEEN THE OPTIONS FOR WHICH FEATURES ARE IMPORTANT?.....	204
TABLE 4.26	PARTICIPANTS' FEEDBACK ABOUT LOCATION VIEWERS PROTOTYPES: LIKEABILITY....	205
TABLE 4.27	PARTICIPANTS' FEEDBACK ABOUT LOCATION VIEWERS PROTOTYPES: DISLIKEABILITY .....	207
TABLE 4.28	PARTICIPANTS' SUGGESTIONS FOR LOCATION VIEWERS FEEDBACK DESIGNS .....	209
TABLE 4.29	QUESTION LIST FOR RATING THE PRIVACY PROTOTYPES. ....	212
TABLE 4.30	ANALYSIS OF RATINGS AS A FUNCTION OF PROTOTYPES (MOOD-TO-MOOD, APPEARANCE-TO- MOOD, APPEARANCE-DIRECTLY).....	213
TABLE 4.31	RANKINGS OF PROTOTYPES.....	214
TABLE 4.32	PARTICIPANTS' FEEDBACK ABOUT VISUAL PRIVACY PROTOTYPES: LIKEABILITY .....	215
TABLE 4.33	PARTICIPANTS' FEEDBACK ABOUT VISUAL PRIVACY PROTOTYPES: DISLIKEABILITY ....	217
TABLE 4.34	PARTICIPANTS' SUGGESTIONS FOR VISUAL PRIVACY AWARENESS DESIGNS .....	218

## LIST OF FIGURES

FIGURE 2.1	A SCREEN CAPTURE OF BROADCASTS CLASSIFICATION OVER WEEK 1. ....	19
FIGURE 2.2	A SCREEN CAPTURE OF BROADCASTS CLASSIFICATION OVER WEEK 2. ....	19
FIGURE 2.3	FACTORS THAT INFLUENCE SELF-DISCLOSURE. ....	25
FIGURE 2.4	A SCREEN CAPTURE OF PEOPLE FINDER APP.....	31
FIGURE 2.5	SOCIAL TRANSLUCENCE FOR BUDDY TRACKER.....	32
FIGURE 2.6	PIXELATING: A VISUAL PRIVACY PROTECTION METHOD.....	36
FIGURE 2.7	AN EXAMPLE OF AN ENCRYPTED IMAGE WHERE THE FACE OF THE PERSON IS CONSIDERED THE SENSITIVE REGION. ....	36
FIGURE 4.1	THE PRIVACY SEAL ICON FOR THE TRUSTE GRANTING AUTHORITY. ....	134
FIGURE 4.2	GEOLOCATE ICON .....	135
FIGURE 4.3	A LIST OF VIEWERS WHO ARE VIEWING THE BROADCASTER’S LOCATION.....	136
FIGURE 4.4	CIRCULAR SLIDING ICONS ARE REPRESENTING VIEWERS WHO ARE VIEWING THE BROADCASTER’S LOCATION AND ARE MOVING TOWARD HIM .....	136
FIGURE 4.5	THE FUNCTIONALITY OF GEOLOCATE PROTOTYPE. ....	138
FIGURE 4.6	GEOWATCH ICON.....	139
FIGURE 4.7	GEOWATCH ICON (INACTIVE MODE) .....	139
FIGURE 4.8	A RADAR PLOT SHOWING THE LOCATION OF VIEWERS WHO ARE CHECKING THE BROADCASTER’S LOCATION.....	140
FIGURE 4.9	THE FUNCTIONALITY OF GEOWATCH PROTOTYPE. ....	142
FIGURE 4.10	GEOBAR GRAPHICAL REPRESENTATION .....	143
FIGURE 4.11	(I) ICON IS SHOWN ONLY WHEN TWO VIEWERS OR MORE LOCATED AT THE SAME LOCATION.....	143
FIGURE 4.12	THE FUNCTIONALITY OF GEOBAR PROTOTYPE.....	145
FIGURE 4.13	FLOWCHART OF MOOD-TO-MOOD TASK FUNCTIONALITY. (A): THE POINT WHERE YOU CAN ENABLE VISUAL PROTECTION. (B): THE POINT WHERE YOU CAN DISABLE VISUAL PROTECTION. ....	151
FIGURE 4.14	MOOD-TO-MOOD PROTOTYPE: THE CASE OF MATCHING HAPPY MOOD.....	152
FIGURE 4.15	METAPHORS OF MOODS USED FOR TASK-BASED AWARENESS DESIGN.....	154
FIGURE 4.16	IMPERFECT METAPHORS FOR THE PURPOSE OF DETECTING DRUNK PEOPLE.....	154

FIGURE 4.17	THE INTERFACE OF MOOD-TO-MOOD TASK.....	155
FIGURE 4.18	A REMINDER AND CONFIRMATION WINDOW ONCE TURNING VISUAL PROTECTION OFF .....	157
FIGURE 4.19	FLOWCHART OF APPEARANCE-TO-MOOD TASK FUNCTIONALITY.....	159
FIGURE 4.20	APPEARANCE-TO MOOD PROTOTYPE. ....	161
FIGURE 4.21	METAPHORS OF MOODS FOR APPEARANCE-TO-MOOD TASK .....	162
FIGURE 4.22	(A) A STANDARD LIVE VIDEO, (B) A BLURRED LIVE VIDEO.....	162
FIGURE 4.23	THE INTERFACE OF APPEARANCE-TO-MOOD TASK.....	163
FIGURE 4.24	FLOWCHART OF CHOOSING YOUR APPEARANCE DIRECTLY TASK.....	165
FIGURE 4.25	CHOOSING YOUR APPEARANCE DIRECTLY TASK PROTOTYPE.....	167
FIGURE 4.26	THE INTERFACE OF CHOOSING YOUR APPEARANCE DIRECTLY TASK. ....	168

## **ABSTRACT**

Many WWW-based live video broadcasting applications (e.g., YouNow, Meerkat, Periscope) do not implement privacy through design. In two studies we gathered information about the current use of such apps, and then designed and tested three prototypes to provide broadcasters with feedback about their viewers and three prototypes to provide mood-based privacy awareness mechanisms.

The first study used an anonymous international English language survey to explore the reasons for use, types of use, knowledge, (privacy) concerns of broadcasters, and desired privacy relevant features of broadcasters who currently use these apps.

Based on key concerns shown in the first study, the first three prototypes of the second study provided information about who had viewed the location of the broadcaster. The second group of three prototypes automatically demonstrates various visual privacy protection methods based on the self-declared mood of the broadcaster. In the second study, three prototypes were designed to provide broadcasters with feedback about viewers who examined the broadcaster's location during a broadcast. Through testing we found 86% of respondents said they would install such apps and 48% would use it regularly. Generally, the best solution would provide more information without intruding on the actual broadcaster. Also, three additional prototypes were designed (and tested) to provide mood-based default privacy settings to help hide inappropriate behavior and then experimentally tested. Fifty-seven percent said they would install such apps, but only 47% said they would use them regularly.

## LIST OF ABBREVIATIONS USED

BCs	BroadCasts
LVB	Live Video Broadcasting
LVFPs	Location Viewers Feedback Prototypes
VPAPs	Visual Privacy Awareness Prototypes
GL	GeoLocate
GW	GeoWatch
GB	GeoBar
MMT	Mood-to-Mood Task
AMT	Appearance-to-Mood
ADT	Appearance Directly Task
ANOVA	Analysis of Variance
$r$	Pearson Correlation
$\Phi$	Phi-Correlation (Coefficient)
$\chi^2$	Chi-Square test
$\eta^2$	Eta-squared (effect size)
SD	Standard Deviation
Min	Minimum
Max	Maximum
$t$	$t$ -tests
$F$	$F$ test (in ANOVA)
$p$	Probability value (as in $\alpha = 0.05$ )
$\alpha$	Alpha Type 1 error rate (as in $\alpha = 0.05$ )

## **ACKNOWLEDGEMENTS**

I would like to thank my supervisor Dr. James Blustein for being so supportive for my research.

I would like also to acknowledge and thank Dr. Brad Frankland for data analysis assistance.

Thanks to Ahmad Alamiri for consultation about designs we used in our study.

I would like to thank Saudi Cultural Bureau for funding this project.

## CHAPTER 1 INTRODUCTION

Social media is defined as “a group of Internet-based applications... which allow the creation and exchange of user-generated content (Stanley, 2015)” with the primary objective of building, developing, and maintaining relationships (Lin & Lu, 2011). It is an important component of many people’s lives, and it is a powerful technology that has been rapidly and widely adopted by people of many ages. The early forms of social media that feature permanent user-generated content, such as Facebook or Twitter, have been widely studied. However, there is a lack of research regarding more modern applications (hereafter “apps”) that do not create permanent material (e.g., Snapchat) in the context of live video broadcasting. Such apps are called *temporal-content social media*, in reference to material that is posted to the Internet but has a finite lifespan, disappearing immediately or after a specified time (O’Reilly, 2007) up to 24 hours.

The general focus of this study is live streaming video mobile apps, such as YouNow<sup>1</sup>, Periscope<sup>2</sup> and Meerkat<sup>3</sup>. Unlike YouTube videos or video chat applications (e.g. Skype), these apps allow a person to post (broadcast) a live video to an unknown public audience on the Internet; after the broadcast ends, the video is gone (Hartsell and Yuen, 2006). Some apps, such as Periscope, have the capability to broadcast the city or exact location of the broadcaster. Periscope is similar to YouNow and Meerkat, but with the ability to display the video for a maximum of 24 hours; it also provides the ability to limit the viewers of the broadcast to a select few, which is called a *private broadcast*. YouNow and Meerkat provide few or no privacy settings, and broadcast to all (called public broadcast) (Dumais, 2015).

Although live video broadcasting is temporary in the case of these types of apps, there are unique issues related to privacy. Since the video is temporarily displayed, broadcasters may assume that privacy is assured, although it is not. Indeed, due to the fact that it is a live video, the broadcaster may be more unguarded and spontaneous than in a planned recording, leading to the

---

<sup>1</sup> <https://younow.com>

<sup>2</sup> <https://periscope.tv>

<sup>3</sup> <http://meerkatapp.co/>



sharing of actions they otherwise might not want to share. Previous research (Wang et al., 2011) found that users often regret posting on social media when they are drunk, angry, or frustrated. Moreover, live video increases the likelihood of violating the privacy of other people who happen to be caught in the video by broadcasting without their permission (as opposed to platforms like YouTube, where material can be pre-screened), possibly resulting in litigation. Broadcasters can also be targets for malicious people, via stalking, ID theft and slander/social ridicule. There are also other concerns related to the unknown audience for a given broadcast. For example, employers might also view such broadcasts, potentially disrupting employer-employee relations and the employer's opinion of their employee. Finally, because of the licensing agreement, the companies that supply these apps may actually capture and use the broadcasts for their own marketing purposes without requiring the broadcaster's explicit permission (e.g., Periscope is owned by Twitter, and Twitter uses this technique with their users' tweets and images) (Pearson, 2015). Hence, there are issues surrounding privacy with these apps. In addition, because Periscope allows the video to be saved temporarily and allows the location in Global Positioning System (GPS) to be shown, there are particularly serious concerns with privacy for Periscope (Pearson, 2015).

In this thesis, privacy and security concerns related to these live broadcasting apps were addressed in two studies, as detailed below. Briefly, we first administered a survey that addresses the lack of existing information related to use of these apps. It did so by asking app users about demographic information, their reasons for using such apps, and their knowledge of and concerns about privacy issues. In the second study, we designed prototypes that address privacy concerns related to disclosure of broadcaster locations and to visual privacy.

## **1.1 Privacy and Privacy Awareness**

Privacy is defined from Oxford English Dictionary (2007) as “The state of being privy to some act”, and the “Absence or avoidance of publicity or display; secrecy, concealment, discretion; protection from public knowledge or availability”. These definitions focus on social and interpersonal perspective. From an information privacy perspective, Westin, a Professor of Public Law & Government Emeritus, Columbia University, former publisher of *Privacy &*

American Business, and former President of the Center for Social & Legal Research, defined privacy as “the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” (Cranor, 2014).

Ackerman, a Professor of Human Computer Interaction and a Professor in the Department of Electrical Engineering and Computer Science and in the School of Information at the University of Michigan, and Mainwaring, a Professor of Political Science, define privacy from interpersonal, social and informational control perspectives as “individuals’ capabilities in a particular social situation to control what they consider to be personal data”. (Ackerman & Mainwaring, 2005; Zhou, 2015)

In this thesis, we address the problem of unawareness of the potential consequences of self-disclosure information or behavior in live video broadcasting, which raises privacy issues mentioned above. The way we address privacy issues in this research is through privacy awareness mechanisms. Therefore, we need to define privacy awareness. Since privacy awareness is not well established in the literature, we adopted the same strategy that Pötzsch (2008) considered in his work to define it. Considering the two perspectives of privacy definitions, which we indicated above, and the meaning of awareness, we can define privacy awareness.

Awareness is about attention, perception and cognition of physical or non-physical objects (Pötzsch, 2008). To achieve the concept of awareness, stimulus that can be either from an environment surrounding the user or from other people are needed (Pötzsch, 2008). Due to the fact that self-disclosure information or behavior occurs through the interaction with people, we use awareness of people stimulus to inform and help the user making a better-informed decision. To this point, privacy awareness can be referred to “the attention, perception and cognition of” (Pötzsch, 2008, p. 228):

- Whether others accessed or have accessed personal information about the user, his/her activities or presence.
- What information they accessed or have accessed in detail.
- How this information has been processed or used.
- What the amount of information about the presence of others and their activities reach to the user and/or interrupt him/her. (Pötzsch, 2008, p. 228)

## 1.2 Overview of Thesis

We examined the problem in two studies. To understand the user privacy perception, we performed an online survey of live video app users. The survey addressed the patterns of, and reasons for, the use of these apps by broadcasters (i.e., users who have created videos, excluding those who have only viewed videos). The survey also addressed the perceptions and use of privacy for broadcasters. We specifically targeted users of YouNow, Meerkat and Periscope, but did not limit participation to those apps (if there should be other apps).

In our follow-up study, we proposed privacy awareness designs as a part of a privacy management system for live video broadcasting apps. This part concerned information that is being disclosed, perhaps inadvertently, by the broadcaster. We used solutions that deal with awareness, detection, and response as parts of privacy management. According to Brunk's privacy framework, privacy management is an ongoing process of awareness, prevention, detection, response and recovery (Zhou, 2015). Almuhimedi et al. (2015) highlighted the effectiveness of privacy nudges in making users aware of privacy risks, and thus help them to make a better-informed decision about their privacy. For example, providing feedback about applications that have access to a user's location made the user change the location settings (Almuhimedi et al., 2015). Jedrzejczyk et al. (2010) confirmed the effectiveness of feedback as a mechanism to reduce privacy concerns. For privacy awareness, we proposed and evaluated a feature that can detect viewers who checked the broadcaster's location then provide a real-time feedback representation of the locations of those viewers. Considering the potential for spontaneous actions or self-disclosure in a live video, we proposed and evaluated privacy awareness mechanism designs for visual privacy protection methods. These methods aimed to address visual privacy issues for broadcasters who are in atypical states (e.g., intoxication) and unaware of potential privacy consequences.

**Specifically, the first study, online survey, addressed the following questions:**

1. How are live streaming video apps currently used?
2. What are the privacy issues associated with that use?
3. What do broadcasters know about the privacy issues of these apps?
4. What do broadcasters want with respect to privacy features?

Our second objective was to consider ways to provide users with better privacy awareness. This includes exploring mechanisms for providing feedback regarding viewer identities and locations in a way that is informative but non-intrusive. The mechanism informs the broadcaster about the movement of viewers when they are around the broadcasting location (e.g., viewers who are moving toward the broadcaster's location). This objective also involves exploration of users' preferences for automatically imposing privacy settings as a function of affective state. The mechanism is also awareness-based solution that either blur or hide the appearance of the broadcaster.

### **1.3 Thesis Structure**

Chapter 1 of this document provides an introduction to the problem at hand, as well as the objectives of the study. Chapter 2 features a literature review, which serves as a foundation of the study. Chapter 3 describes the survey methodology and discusses the results, outlining the limitations and future work, while Chapter 4 explores the proposal designs for privacy awareness mechanisms and presents the outcome of the design evaluation study, highlighting the design guidelines, the study limitations and future work. Chapter 5 provides the conclusion, contribution of the thesis, an overview of the limitation and future directions for this line of research.

## CHAPTER 2 LITERATURE REVIEW

In recent years, users around the world have become increasingly connected through social media (Facebook, Twitter, etc.), with nearly every aspect of their lives being affected in some ways by such technology. Videos, which constitute one of the major forms of social interaction, exist in both recorded forms (e.g., YouTube) and in instantaneous forms, usually but not always in a private, face-to-face context (e.g., Skype, Facetime). The type and magnitude of privacy issues vary across these distinct types of videos.

Live video broadcasting represents one of the most popular emerging forms of social media, and possibly the one most fraught with privacy concerns. With the aid of rapidly advancing technology, live videos have been recently adopted by users of different ages as part of a new form of social media, temporal or self-destructing or so-called “ephemeral” social media. Unlike more traditional social media, live video broadcasting apps present the broadcaster not through a profile on a page or wall but rather through the videos themselves – based on the broadcaster’s words, behaviour, personality, and reactions. In putting a higher emphasis on self-monitoring, it likely attracts a different subset of users than other forms. Similarly, its temporal nature likely leads to different patterns of usage.

This new form of media raises unique privacy concerns for several reasons. For one, unlike YouTube, Vine, and others, these videos are spontaneous, playing in real time and therefore making certain aspects of moderation impossible. Related to the fact that the videos are live, it is also difficult for the broadcaster to be certain of the audience that is watching – and perhaps recording – their transmission. Thus, the usage of apps that facilitate live video transmission come with their own emerging privacy issues that require special attention in order to preserve user privacy. The literature review that follows will first discuss research related to social media in general. It will then discuss social media forms that use video, addressing the related privacy concerns. The review will also discuss live video in particular, with special attention to its unique privacy issues.

## 2.1 An Overview of Social Media

### 2.1.1 Use and Impacts of Social Media

Social media is a cyber environment where people exchange information, in the forms of text, photos, and videos, and build and/or maintain relationships. Especially given the increasing prevalence of social media, it is important to understand who adopts it, and why. One of the most common psychology models used to understand people's difference in personality is "*The Big 5 personality model*" or called "*Five factor model*". This model includes the following dimensions; Extroversion ("*the extent to which someone is outgoing and enjoy socializing*"), Emotional stability ("*the extent to which someone is stable versus neurotic, insecure, or nervous*"), Openness to new experience ("*the extent to which someone seeks intellectual stimulation*"), Conscientiousness ("*the extent to which someone is organized or self-disciplined*"), and Agreeableness ("*the extent to which someone is compassionate or empathetic*") (Egelman & Peer, 2015). This model is developed as part of Personal Behavior theory (Egelman & Peer, 2015). Previous studies found that the three of these five dimensions that are relevant to the use of online social application are extroversion, emotional instability, and openness to new experience (Correa, Hinsley & De Zuniga, 2010).

Early studies found that introversion and neuroticism, *related to loneliness*, are the most personal traits that characterize the frequent users of online activities (Correa et al., 2010). Considering gender differences, women who feel loneliness and neuroticism are more active in online chat and group discussion than men (Hamburger & Ben-Artzi, 2000; Correa et al., 2010). The reason is that the anonymity of the Internet attracts those who have difficulties making connections with others (Amichai-Hamburger, Wainapel & Fox 2002; Correa et al., 2010). However, recent studies indicate that people who are extroverted are more frequently using social network sites and instant messages because usually users who intend to use these technologies are more likely to use them for the purpose of connecting with familiar people (e.g., friends, family) (Correa et al., 2010). Correa et al. (2010) indicate that the three of the five attributes in the classic Big Five Personality Model are predictive of social media use: extroversion and openness are positively correlated with social media use, while emotional stability is negatively correlated with social media use. It is important to note that Correa et al.,

(2010) in their research, defined social media as “social networking sites and instant messages”. These findings imply that the relationship between personality traits and social media use differ depending on the type and nature of social media interaction.

Extroverted and neurotic people are appealed by specific types of social media. Usually extroverted people seemed to make connections with other people in social network sites and also in their real life (Zywica & Danowski, 2008; Correa et al., 2010). Ellison et al. (2007) found that social network sites could be a good alternative for people who have less of esteem or less life satisfied (Correa et al., 2010). However, neurotic people were more attracted with instant messaging instead of face-to face interaction (Ehrenberg et al., 2008; Correa et al., 2010). This is likely because instant messaging provides enough time to the user to think about the response before the actual response (Ehrenberg et al., 2008; Correa et al., 2010). Moreover, most social network users reported their curiosity or openness to new experience (Ross et al., 2009).

The profile of social media users may differ with respect to live video broadcasting apps, mainly because of the spontaneity and non-anonymity in live videos, which may appeal to those who are impulsive and/or emotionally unstable. There is a need for more research investigating the particular personality traits that characterize users of temporal or “ephemeral” social media, as well as the kinds of activities that people undertake in live videos – and whether these activities bring about adverse consequences.

Although social media usage differs greatly from one user to the next, research has detected some consistent patterns in the way people use it. Employing social capital theory to classify the use of social media (Pfeil, Arjan & Zaphiris, 2009), researchers have determined that people use social media either for bridging or bonding. Bridging implies weak ties with others that does not involve the sharing of sensitive or personal information, whereas bonding involves strong ties that involves exchanging such information and seeking support (Pfeil et al., 2009). Similarly, Kuss and Griffiths (2011) found that most users engage in social media for the purpose of making or maintaining a relationship. Studies of how usage differs with gender and age have detected difference between men and women (Kuss & Griffiths, 2011). Some studies found that men seem to make friendship on social media more than women (Raacke & Bonds-Raacke, 2008) , but other studies found the opposite (Pfeil et al., 2009). In addition, men tend to disclose more personal information than women (Kuss & Griffiths, 2011). Research on age indicates that teenagers make friends with those of similar age, and also that they develop larger

networks than older people (Pfeil et al., 2009; Kuss & Griffiths, 2011). Younger users also tend to carefully use their profiles to form distinctive identities and attract users. More than young users, older people use social media to communicate online with people from different countries, culture, and ages. They also use it to explore news, events and information (Pfeil et al., 2009). According to an online survey of psychology students in the US, the most common activities on social media are reading or responding to comments or posting on someone's pages (60%), sending messages or invitations (14%), and browsing others' profiles (13%). Also, it was found that social searching activity (extracting information from someone's profile) is more enjoyable than social browsing (randomly exploring news feeds) (Kuss & Griffiths, 2011). More importantly, culture has an impact on usage as Western is more self-disclosure than Asian and Eastern cultures (Misoch, 2014).

Other researchers have also explored the factors motivating people to use social media. Using motivation theory, Lin and Lu (2011) found that two common reasons relate to the usefulness of social media and the enjoyment derived from it. In particular, enjoyment is a motivation for pleasurable-oriented information systems (e.g., social networks or games systems), and usefulness is a motivation for task-oriented information systems (e.g., business-based systems). Researchers who applied network externalities theory found that people also use social media on the basis of positive word-of-mouth from friends and relatives (Widjaja et al., 2012; Beldad & Kusumadewi, 2015; & Lu, 2011). Furthermore, Lin and Lu (2011) found that women are more affected by the magnitude of peers' feedback regarding usefulness and enjoyment, whereas men are affected by the number of peers using it and perceived reputation of the platform. On the other hand, users with high social identity use it because of the compliments and attention that they obtain from other users of the social network (Kuss & Griffiths, 2011). A study of university students revealed the following reasons: maintaining relationships with people they do not see frequently (81% of respondents), because their friends have accounts (61%), contacting relatives (48%), and making plans with people that they often see (35%) (Subrahmanyam et al., 2008; Kuss & Griffiths, 2011); some are also driven by the desire to communicate via social media rather than doing so through face-to-face interaction (Kuss & Griffiths, 2011; Kujath, 2011).

Although social media can aid greatly in activities like starting businesses, seeking advice, and exchanging information (Ngai et al., 2015), its prevalent usage has wide-ranging



effects that play out on individual, organizational, and social levels. In particular, the degree of sharing of personal information leads to such information being widely disclosed (Ngai et al., 2015), posing a great threat to the private life and, in some cases, the safety of the individual. In addition, an individual is more likely to be exposed to cyberbullying (e.g. harassment, threatening, cyberstalking, making jokes or fun of etc.) (Slonje et al., 2013) through social media, leading to negative effects on one's mental health (Ngai et al., 2015). Similarly, negative feedback occurs more commonly online than in real life; this may negatively impact low self-esteem people who use social media as an alternative to real life (Kuss & Griffiths, 2011). From an organizational perspective, employees may have difficulties differentiating between professional and personal life when using social media (Ngai et al., 2015). While social media is valuable to use for communication by people who are physically or socially restricted, it has the potential to reduce the level of real life communication for most users (Ngai et al., 2015). Particularly, people have tended to rely on social media in marketing either for big or small business to reach wide customers from different parts of the world, or for buying products, or for outreach for the purpose of advocating for change.

The sorts of negative effects associated with traditional forms of social media, may also take place with live video streaming apps. The impact of such effects might even be greater in this case, simply because of the increased level of anonymity of the viewers – and increased level of uncertainty about who is watching – for the broadcaster (Slonje et al., 2013). Indeed, because the interaction between the broadcasters and the viewers on live video broadcasting is through text chatting, the viewers can retain complete anonymity if they choose. This arrangement, where one party is anonymous but the other is not, is unique to this type of social media and can lead to a negative reputation for the individual user, along with all of the negative consequences that result.

The factors motivating individuals to use newly emerging live video broadcasting applications are less clear and require research attention. In the following sections, we will explore in greater detail the various types of social media that rely upon video.

### **2.1.2 The Emergence of Video in Social Media**

Forms of social media with video components may involve either pre-recorded media or video

streaming. Pre-recorded media (e.g., YouTube videos) can take a long time to play due to its large size when downloading. In contrast, *video streaming* is a technique that involves compression and buffering live video while transmitting and real-time viewing the video (Hartsell & Yuen, 2006). In the case of streaming (e.g., Periscope videos), the video is downloaded, transmitted and displayed simultaneously through the server application to the client application. Closing the client-side application causes the video to be deleted automatically from the user's device (Hartsell & Yuen, 2006). Below, I will discuss the various forms of social media related to files recorded (pre-recorded media) and streaming video.

## *YouTube*

The most established and popular video platform is YouTube, which allows its users “to watch or to upload videos, to share content, to subscribe to channels, to comment or to rate videos” (Misoch, 2014). Rather than being streamed, YouTube videos are video files that can be classified into two types: videos created by users to be shared via YouTube, and videos featuring content copied from movies, TV shows, and other preexisting sources (Ding et al., 2011). A study of the target audience for videos identified three types of audiences: the identified-offline public, who has some connection to the uploader (e.g., family member); the identified-online public, who are unfamiliar to the uploader but share similar interests; and the unidentified-online public who represent the remainder of the general public (Courtois et al., 2013). Uploaders were asked about their reasons for trying to connect to these audiences; their objectives included showing skills and simply reaching the largest portion of the Internet audience possible (Courtois et al., 2013). Based on the targeted audiences identified, we can conclude that YouTube videos are exposed to these people, which implies that these uploaders are less likely to upload videos that include personal sensitive information. In other words, they do not have high privacy concerns because, with YouTube videos, a user can edit or trim unwanted parts of videos, eliminating unwanted personal disclosures before posting it to the public (Misoch, 2015). Therefore, self-disclosure in YouTube videos should be considered differently from self-disclosure in real-time videos.

## *Video Chat*

Differing from YouTube in that they rely on streaming video, video chat applications (e.g.,

Skype, Facetime, MSN Window Messenger, etc.) are used mainly for live communications among people who have strong ties relationships (e.g., friends, family) but live far away from each other (Judge & Neustaedter, 2010; Massimi & Neustaedter, 2014; Wang, Mughal & Juhlin, 2015) and users can see each other while chatting. Activities during these chats can either be focused on specific activities (e.g. showing clothes, cooking, personal achievements, gossip) (O'Hara, Black & Lipson, 2006) or can involve more open-ended interactions (e.g. performing, multiple conversations, homework) (Judge & Neustaedter, 2010; Buhler, Neustaedter & Hillman, 2013). Such video platforms can also be used in the workplace, allowing for online meetings among people working in different places, even if it is just different offices within the same geographical region (Massimi & Neustaedter, 2014). Another application of this kind of video chat is for special events (e.g., wedding, graduation, funeral) where some people (e.g., friends and relatives) are unable to attend (Neustaedter et al., 2015). This kind of situation may occur for several reasons (Massimi & Neustaedter, 2014). For example, guests who live remotely sometimes cannot come in person to the event because of expensive tickets, busy schedules, or health reasons (Massimi & Neustaedter, 2014) (Neustaedter et al., 2015). Nonetheless, some participants strongly disagreed with the idea of using video chat for personal events (e.g., child birth) (Massimi & Neustaedter, 2014). Because video chat is mainly used for communication with friends and families, there are relatively few privacy concerns (Judge & Neustaedter, 2010; Massimi & Neustaedter, 2014). Nonetheless, there are some, teenagers may have concerns about unclean rooms or their personal appearances, as well as concerns about being overheard by parents or others in the area (Buhler et al., 2013). Previous studies have indicated that, while overall privacy concerns are low with these platforms, there are some concerns about interruption, autonomy, and information being accidentally revealed to unintended audiences (Judge & Neustaedter, 2010). In the case of workplace use, there are some concerns about knowing with certainty who is seeing the video and about some people not being aware that they are on camera (Massimi & Neustaedter, 2014). Participants in (Massimi & Neustaedter, 2014) who use video chat for major events in their lives do not report any privacy concerns, such as recording others without others' permissions or how good their appearance is. Indeed, some participants suggested the idea of recording video chat for later replay. However, recording video chat transfers the nature of streamed video to permanent video, which could lead to novel unwanted consequences for those participating in the event (Massimi & Neustaedter, 2014), and

violate their privacy.

### ***Live video Broadcasting***

Live video broadcasting is typically used for transmitting real-time videos to any and all possible viewers, but the broadcaster cannot see the viewers. The emergence of live video broadcast was with the use of desktop webcasting where a webcam was used to broadcast to a website (Shamma et al., 2009). However, this required the user to be in a fixed place, making an obstacle to those who want to broadcast outside a specific location such as outdoors. In such cases, previously, users can record a video using DV camera or camera that is embedded in mobile phone, and then send it to a website (Juhlin, Engström & Reponen, 2010), which is similar to the idea of YouTube videos. Then, the technology of mobile webcasting evolved that is closely derived from video conferencing systems (O'Hara et al., 2006). The type of interaction that distinguishes between the two were having unlimited audience with non-face-to-face interaction characterize mobile webcasting versus limited number of audience with the possibility of face-to-face interaction in video conferencing systems (Juhlin et al., 2010). Mobile webcasting is implemented from mobile phone to a public website. The first service that applied this technology was ComVu Pocket Caster, which was launched in 2005, and renamed later as LiveCast (Reponen, 2008). Other similar applications evolved after that (e.g., Stickam, Ustream, etc.) and they share common characteristics, such as ability to view broadcasts later, sharing broadcasts with other webpages, or email, live chatting and/or commenting (Juhlin et al., 2010). The common contents of these broadcasts were mostly professional, such as landscape, public places, or testing technology (Juhlin et al., 2010). The purpose for broadcasting was for maintaining connection with others, showing performance, or having fans (Juhlin et al., 2010).

The equipment used for live video broadcasts may include desktop video streaming, website and mobile video conferencing system (e.g. webcam or fixed-video camera) (Juhlin et al., 2010), or mobile video camera embedded on a cell phone with the use of a mobile application (Landgren & Bergstrand, 2010). However, having a mobile app to broadcast live videos is more flexible as users can broadcast whenever and wherever they are (Landgren & Bergstrand, 2010). Based on video content analysis of webcam broadcasts, the most common types of video broadcast are the technology test and demonstration. *Technology test* is where the user displays interiors (e.g., apartment), and the camera unsteadily moving especially at the start

and end of the broadcast. In this case the attention is on handset interface rather than broadcast content. *Demonstration* is where the user explains how technology works to friends, family or colleagues (Juhlin et al., 2010). Other common types include broadcasts about tours, performances and presentations, social events, group and family events, landscapes, TV, computer screens and sharing spontaneous moments (Juhlin et al., 2010). On the other hand, the benefit of mobile live videos can be seen in several situations, such as formal documentation, training, and learning activities. It can also be valuable in an emergency case where authorities can see what and where something is happening. In such cases, the video would provide the opportunity to control and decide remotely what help is needed at the moment and whether there is a need to change the plan (Landgren & Bergstrand, 2010).

Privacy concerns have not been reported in the literature when using webcam broadcasting (webcasting) in conference or large meetings (Massimi & Neustaedter, 2014), but the situation is different when individuals are broadcasting informally and when the number of people participating in a broadcast is highly variable, as well as other settings may differ (Massimi & Neustaedter, 2014).

### **2.1.3 Temporal Social Media (Live Video Broadcasting)**

The newly emerging area of temporal social media differs from both recorded video platforms such as YouTube and streaming platforms such as Skype in that the video content remains viewable for a specific amount of time prior to being automatically deleted. This contrasts with more traditional forms, wherein “social media has the attribute of permanent content” (Stanley, 2015). Examples of temporal social media apps, which trade in this so-called ephemeral data (Shein, 2013), include Snapchat, Slingshor, Snapper, Wickr, and Periscope. Such apps are becoming increasingly popular, in part because they provide more control over media exchange, and therefore more control over how one’s personal life disclosed (Stanley, 2015). Another reason is because users believe that the content will not be permanently available for viewing, so “[the users] can be their real selves...because it’s not there forever.” (Shein, 2013). With self-destructing forms of social media, people tend to think less carefully about how an online activity may negatively affect them at a personal level (Mayer-Schönberger, 2011). One of these apps’ most appealing aspects from the user’s perspective is that users can send secretive content

in a way that minimizes the amount of data that other parties have about them. Snapchat, a popular time-limited instant messaging service (Piwek & Joinson, 2016), is frequently used for sending photos or videos of funny things that happen in the moment to friends (Shein, 2013). While the chief appeal lies in the ephemeral nature of the media, the content can be captured. For example, the user receiving the content may take screenshots of photos or videos or by recording the received video using either another camera (Stanley, 2015), third party apps or other advanced tools (Khan, Mashiane & Shozi, 2015). Thus, temporal social media apps are not necessarily as safe as they may seem, with potential privacy issues that users may not realize when they engage in sharing photos or video. As with temporal photo/recorded video apps, temporal live video streaming apps embrace the concept of self-destructing content. Topics in temporal live video broadcast range from serious to causal discussion (Dumais, 2015). Three live video broadcasting apps, YouNow, Meerkat and Periscope, were chosen for examination in this study because of the similarities and differences they have: YouNow and Meerkat both delete the live broadcast immediately once a broadcaster ends his video. However, Periscope provides an additional option for a broadcaster to make the video available to be viewed by others for up to 24 hours after broadcasting (Pierce, 2015). Also, Meerkat and YouNow are restricted to public broadcasting, such that anyone on the Internet can see the broadcast; in contrast, Periscope offers public broadcasting as well as narrowcasting, in which the broadcaster can select exactly who can view the video (Pierce, 2015). Each of the three apps is introduced in more detail below.

YouNow, is a live video webcast that was launched in 2011, making it the oldest live video streaming app (All Things Digital, 2013). Its popularity increased during 2014 and 2015 (Jarvey, 2015) after updating the service with changes (Kafka, 2014). In 2013, YouNow bought, Blog tv, a live streaming-video website that uses webcams for broadcasting, and Blog tv's users incorporated into YouNow (Kafka, 2014). YouNow is mainly used to support talented individuals who show their skills, with broadcasters able to earn money through their partnerships with YouNow (Jarvey, 2015). Viewers can donate virtual gold bars if they admire the skills of the broadcaster (Kafka, 2014; LeSure, 2015), with 60% of the money going to the broadcaster (Flynn, 2016). Currently, YouNow can be used on a desktop or as a mobile app, and broadcasts are categorized by trending topics (e.g., using hash tags). The app also provides other features, such as chatting, sending likes and stickers (LeSure, 2015). In terms of privacy, a user can hide the city where he is located, block or flag someone, and use a nickname instead of a real

name (Dumais, 2015).

Meerkat, developed by the tech company Life on Air, a team led by Ben Rubin (Geier, 2015), and was released in February 2015 and integrated with Twitter. Meerkat does not provide its own timeline or profile for broadcasters (Weil, 2015). Instead, whenever a user writes a comment on a broadcast, the comment is shown on the user's Twitter feed (Dumais, 2015). This feature may be annoying to some participants because it provides an impression to others about the type of conversation that occurred at that time (Hachman, 2015). Celebrities, brands, strangers and twitter followers comprise the audience for Meerkat. Meerkat has two main options for broadcasting: The stream option allows the broadcaster to immediately broadcast the live video to the world, while the schedule option enables a broadcaster to pre-record their live video and then broadcast it at a specified time (Hachman, 2015). Viewers can benefit from this feature to learn about upcoming broadcasts (Dumais, 2015).

Periscope is a real-time video-broadcasting mobile app that developed by Kayvon Beykpour and Joe Bernstein, and purchased by Twitter in March 2015 (Weil, 2015; Shontell, 2015). After acquiring Periscope, Twitter blocked Meerkat from accessing Twitter followers because the companies were no longer partners. As a result, when any user joins Meerkat, their Twitter followers are not notified that he/she has joined Meerkat (Pierce, 2015; Pullen, 2015). The idea of Periscope originated during the summer of 2013 when Kayvon Beykpour, who was planning to travel to Turkey, was concerned by news of a protest taking place near the hotel where he would be staying. He was unable to find useful information on TV or Twitter, leading him to think about how he would be able to see what people there were seeing if those people could use their mobile phones with high speed data plans in order to broadcast (Pierce, 2015).

Periscope has a number of special features including private and public broadcasts (Pierce, 2015). It also enables the viewers to tap colored hearts on the screen (Weil, 2015) to show 'likes' for particular broadcasts. Also, Periscope enables the broadcaster to save the broadcast on his device or gallery (Periscope Help Centre, 2016), and to block or report broadcasts for abuse (Pierce, 2015). In addition, there is a global list or map that shows the precise location of public broadcasts taking place at a given time, with such information remaining public up to 24 hours (Weil, 2015). Periscope profiles show who a given user is following and followed by, as well as a list of recent broadcasts initiated (Weil, 2015). Although Twitter owns Periscope, Periscope is independent from Twitter, with engagement on Periscope

not shown on users' Twitter feeds (Pullen, 2015). However, Twitter followers get notified when a broadcaster they follow starts broadcasting (Pierce, 2015); likewise, it is not necessary to sign up for a new account for Periscope, as users can use their Twitter accounts as a Periscope account. The context of broadcasts varies from public (e.g., lectures) to personal events (e.g., parties) from silent (e.g., not talking at all) to explaining what is happening or head talks (a user facing his mobile phone (showing the upper part of body and having a talk (Massimi and Neustaedter, 2014)) (Segall, 2015).

### ***Periscope Broadcasts Contents***

This section describes the geographical distribution of Periscope broadcasts, as well as the types of live video that are most commonly broadcast by Periscope users. It is based on personal observations of Periscope content over a period of one month, two times a day, in the afternoon and night as well as information from Dextro, a computer vision company that dynamically scans and categorizes live video content from Periscope into trending themes for brands, objects and scenes (Dextro, 2015). To further characterize the breadth of Periscope use, this report also includes a Periscope-related incident reported by CBC News.

Using Periscope's "Map tab", we determined that the areas producing the most public broadcasts were the United States and Europe, followed by South America. There were relatively few broadcasters in countries in the Gulf of Arabia and even fewer broadcasters in Canada. Daytime hours may contribute to the change.

Based on personal observation, the broadcasts on Periscope could be classified into the following groups:

1. Formal Presentations: Many users broadcast others while they talking in front of general public and/or specific people discussing religious topics (e.g., "State of Church Planting Research", "Good or God", and events such as the pope's visit to Philadelphia). There were also a number of political conferences and interviews (e.g., "Press Avail after homeschool meet & greet un Urbandale", RCYM youth conference and class lectures). Some known companies' leaders or workers also produced broadcasts (e.g., "Taking uneatable [sic] live with guests by Bell Lawrence", "Intel booth tour at World #MakerFaire #NYC").
2. Personal talking: Many of the broadcasts feature a user talking about himself/herself, often asking known or unknown users to ask him/her any question they want via chat. Examples



of broadcast titles include “So bored ask questions”, “ask me any question”, “drinking and answering questions”, “Off work”, “On campus”, “ask anything”, “ask us anything: take two”. These broadcasts are performed mostly at home or while driving, and typically display the broadcaster’s precise location; many broadcast while they are drunk, particularly on the weekend. In addition, there are users who broadcast to seek advice or support, or advocate for causes (e.g. “Help protecting kids. Risk point”, “Just need motivation for homework”, “My goal to find a cure for cancer”, “My kid know more about tech than I do”)

3. Activities: Many broadcast while doing activities, such as playing games, walking, cooking, and driving (broadcast titles include “Basketball on arena”, “University of Kentucky volleyball post game interview after 3-0 win over Hatfold”, “Firefighters common post bar in Emmitsburg”, “Tour of Calvary”, “walking around Bayside in Miami take”, “Vegas night”). There were also many sexual activities and jokes broadcasted.
4. Events: a number of broadcasted showed events such as parties, concerts, and wedding receptions.

Dextro (2015) classifies broadcasts into the following topics on a weekly basis:

- Talking heads
- People/Crowds
- Computer
- Nightclub & Concert
- Watching TV
- Glasses: the vision system recognizes any material that contain glass.
- Musicians
- Cats & dogs
- Dashcam
- It’s Getting Dark: the vision system recognizes dark places.
- Fridge Tour: the vision system recognizes fridges when people broadcast moving the camera around the fridge.

The most common topic on Periscope is “Talking heads”, with 80,344 - 77,236 broadcasts over two weeks. Then, the next most popular topic is People/crowd, with 43,344 - 42,097 broadcasts. These were followed by broadcasts about computers (14,490 - 11,660) and Nightclub & Concert (5,827 - 5,787) (see Figures 2.1 and 2.2).

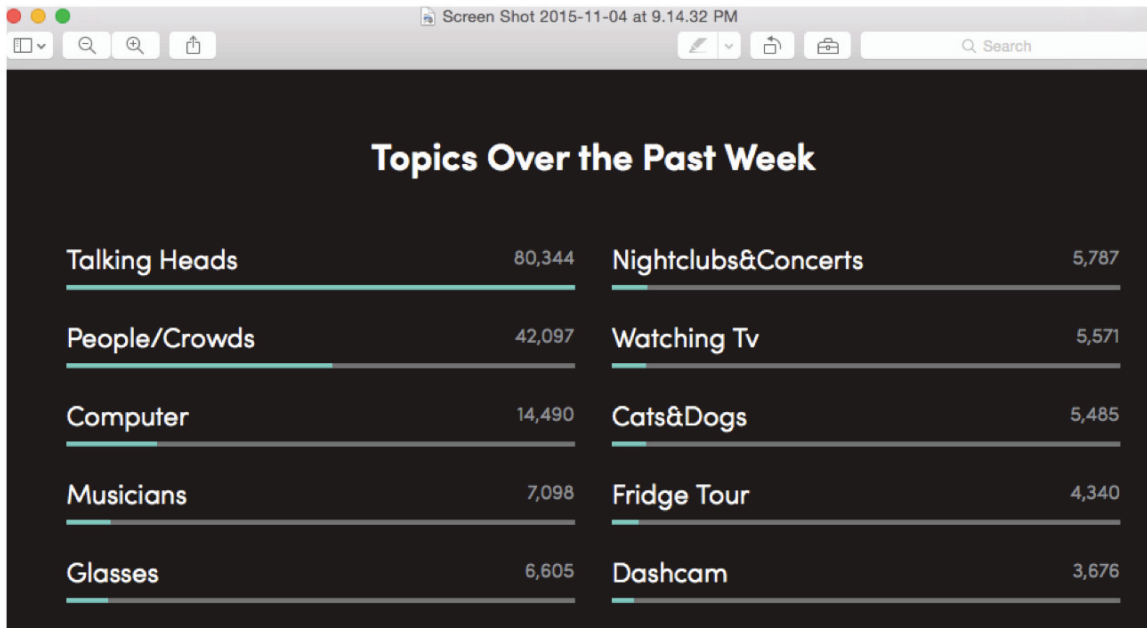


Figure 2.1 A screen capture of broadcasts classification over week 1. Retrieved from (Dextro, 2015)

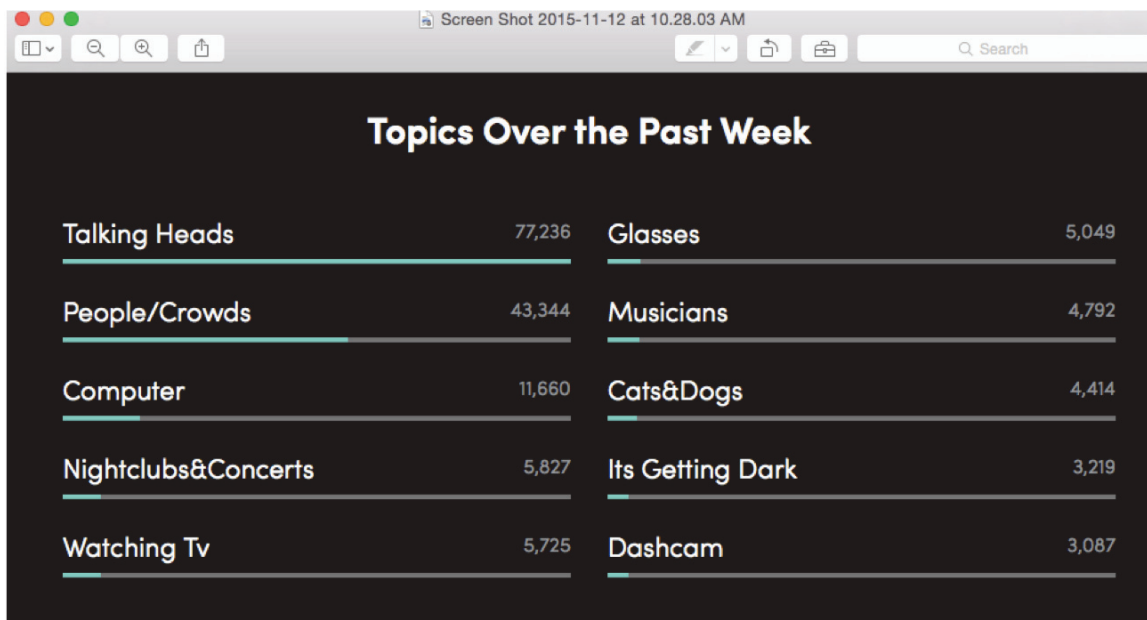


Figure 2.2 A screen capture of broadcasts classification over week 2. Retrieved from (Dextro, 2015)

While many Periscope broadcasts cover familiar topics, sometimes broadcasts extend into unique and occasionally controversial territory. For example, on Oct 13, 2015 CNN News reported the story, “Woman live streams herself while driving drunk, police say”. She was 23 years old and she was broadcasting on Periscope at the bar with the title “Drunk people at the bar”. After she got out from the bar, she broadcasted again, and the title of the broadcast was “Driving home drunk”. She was not aware of where she was, so she was asking the viewers on periscope; she was also concerned that one of her tires was flat. One of the viewers called 911 and reported that he just saw a young girl streaming live video on Periscope while drunk driving. Police in Lakeland, Florida arrested her and she was charged with driving under the influence of alcohol, which she admitted. Her attorney confirmed that she was unwilling to give any interview, stating that “she is a young professional with a bright future” and that he would “be entering a plea on her behalf of not guilty”. The police was thankful that she did not cause an accident or damage, stating, “The streaming Periscope video highlights the dangers of driving while intoxicated.” (Ford, 2015).

From this incident, there are some points should be highlighted. While Periscope was helpful in the case of rescuing the woman from danger, it is not always the case. There might be malicious people who could see her on Periscope and track her using knowledge of her precise location. Another issue is the impression she creates with her behavior, given her attorney’s characterization of her having a “bright future”. This incident is a good example of how privacy issues can impact users, and that such issues should be addressed in order to protect the user privacy.

## **2.2 Privacy and Self-Disclosure of Information**

Two main areas of privacy in media space have been discussed; access control (e.g., authorization) and content privacy (e.g., deleting personal information from platforms). Meaning that these areas rely either on technical-based solutions and/or warning or awareness-based solutions (AlSagri & AlAboodi, 2015). In the context of live video broadcasting as a social medium, broadcasters are expected to unknowingly disclose information while interacting with others. Due to the nature of spontaneous live video, we focus on awareness-based solutions.

Self-disclosure is defined as “the act of revealing personal information to others, in the proper sense, when it concerns a person’s own information” (Misoch, 2015, p. 535). Parameters controlling self-disclosure include the amount of information revealed (breadth) the level of privacy (depth) (Misoch, 2014; LeSure, 2015), and the amount of time spent on revealing information (Misoch, 2014; LeSure, 2015). While breadth and depth are both important for promoting intimate relationships (Misoch, 2014; LeSure, 2015), they differ in important respects. Breadth is more concentrated on external characteristics (e.g., occupation and preferences), whereas depth is more related to internal or sensitive characteristics that usually hidden from others (LeSure, 2015). Previous studies investigated the reasons for users’ privacy disclosure using privacy calculus models under exchange theory, and found that users tend to disclose personal information in social media in order to gain perceived benefits, suggesting that users make rational decisions in information disclosure (Dinev & Hart, 2006; LeSure, 2015). Other studies found that self-disclosure is determined by the sensitivity of the personal information in question (Nowak and Phelps, 1997; Phelps, Nowak & Ferrell, 2000; LeSure, 2015). However, users are not always aware of their own behavior with regard to self-disclosure (Acquisti & Grossklags, 2003; LeSure, 2015), especially in real-time videos situations.

### **2.2.1 Factors Influencing Privacy and Self-Disclosure**

A review of empirical research on privacy behavior conducted within the social and behavioral sciences highlights three themes: uncertainty, context-dependence, and “malleability” and influence (Acquisti, Brandimarte & Loewenstein, 2015). In terms of uncertainty, users commonly possess doubts about how much information they should share and even whether or not they should have privacy concerns. It is not surprising that users have little sense of the consequences of their sharing, given that advanced information technology does not clearly show the user what information is collected and how it is used. In addition, users are often uncertain of their privacy preferences (Acquisti et al., 2015). Related to that, a study by Westin classified users in terms of privacy into three categories based on general survey about privacy: privacy fundamentalists, pragmatists, or unconcerned (Acquisti et al., 2015). However, when asked directly, most users were privacy fundamentalists. This contradiction, called the privacy paradox (Acquisti et al., 2015), indicates that attitude does not always predict actual behavior.

Another study surveyed participants about their attitude toward sharing information and then provided “a product to purchase at a discount with the assistance of an anthropomorphic shopping agent” (Spiekermann, Grossklags & Berendt, 2001). Few of the participants refused to answer the sensitive questions that the agent asked them, indicating that people claim they care about privacy but often behave differently. One possible explanation is that users may consider the costs and benefits associated with a given situation (Acquisti et al., 2015). Indeed, this kind of decision-making is probably an important factor influencing privacy behavior, along with emotions, social norms, heuristics, and misconceptions related to costs and benefits (Acquisti et al., 2015).

This leads to the second theme of privacy behavior research, context-dependence (Acquisti et al., 2015), which means that an individual’s concerns over privacy can vary widely depending on the situation. (Acquisti et al., 2015). According to Westin, any of us may be a privacy fundamentalist, a privacy pragmatist or unconcerned about privacy depending on the given time and place (Acquisti et al., 2015). Therefore, users manage their privacy rules based on situational, cultural and motivational factors, and these rules are learned over time. In fact, users refer to cues to judge about their privacy importance (Acquisti et al., 2015). For example, it was found that the existence of government regulations positively influences user behavior in terms of disclosing more information because it increases the user’s trust in the disclosure process (Acquisti et al., 2015). However, sometimes cues can be unrelated or negatively related to the standard behavior of decision-making. For example, a study found that users reveal more personal and incriminating information when interacting with an unprofessional website with a title “How Bad R U?”, as compared to a more formal interface (Acquisti et al., 2015). The physical environment is another cue that “influences concerns and associated behavior” (Acquisti et al., 2015). For instance, people tend to be engaging in more self-disclosure when they are sitting in a warm room with soft lighting than when they are in a cold room that has strong lighting (Altman, 1975). The culture and behavior of others also plays a role, particularly in the case of intimation and reciprocity. Such factors tend to increase the amount of self-disclosure behavior, mainly because revealing one’s information increases the possibility of the other party revealing his or her own information without much thought (Acquisti et al., 2015). Research indicates that one’s behavior can be strongly influenced by the behaviors of other users (Petronio, 2012). For example, a user on Facebook blocked his friend from seeing his profile

after his friend revealed it to an unintended audience (Stutzman & Kramer-Duffield, 2010). Another cue is past experience; for example, knowing that a place recently added surveillance increases privacy concerns (Acquisti et al., 2015).

The third theme is the “malleability of privacy preferences”, which relates to the factors that either activate privacy concerns or lessen them (Acquisti et al., 2015). The tools to achieve such malleability of privacy preferences include using default settings to affect behavior and helping to make users’ decisions regarding privacy behavior (Acquisti et al., 2015). Another possible tool is designing system features that frustrate or confuse the user into disclosing personal information; this method is called “malicious interface design” (Conti & Sobiesk, 2010; Acquisti et al., 2015). Similarly yet less malicious, simply giving users the power to manage their own privacy can reduce privacy concerns, yet actually have unintended effects upon disclosure via increased trust levels (Acquisti et al., 2015).

### **2.2.2 Privacy and Self-Disclosure in Social Media**

Some researchers have specifically investigated issues of privacy and self-disclosure in the context of social media and, in particular, video platforms. For example, Misoch (2015) proposed a model describing factors involved in online self-disclosure, based on YouTube videos analysis (see figure 2.3). The study found that whether one is sitting alone or with group of people in front of a screen makes a large difference the amount of information disclosure. In particular, a user is more likely to reveal more personal information and provide a more extensive self-report when alone, unhindered by the self-consciousness associated with being in a group (Joinson, 1999; Misoch, 2014; Misoch, 2015). In addition, communicating through a computer leads to lower levels of *social presence*, which relates to how noticeable, or visible, one is within social interactions. Lower levels of social presence, in turn, induce more self-disclosure and can lead to undesirable social behavior (Misoch, 2014; Misoch, 2015). In our study, we assume that the user is broadcasting alone, not with a group who know they are on a live video. However, others, who are surrounding the broadcaster and who they do not know about broadcasting, might be caught on the broadcast.

Furthermore, the channel characteristics used for communication affect self-disclosure, whether with textual, visual-audio (Misoch, 2015) or visual-textual exchanges, and can develop

or limit self-disclosure. The degree of self-disclosure is, not surprisingly, influenced by factors such as the motivation for communicating, emotional or personal characteristics (e.g., loneliness, life satisfaction, and health) (Misoch, 2015), and cultural differences (Goh, 2011; Misoch, 2015) (e.g., Western users disclose more than others) (Chen, 1992; Misoch, 2015). In terms of gender, the results of research are unclear: while some studies suggest that women disclose more than men (Trammell et al., 2006; Misoch, 2015), other studies found no difference (Cho, 2007; Misoch, 2015). Some studies indicate that young users disclose more personal information than older people, likely because they are more invested in such new technologies (Wang, Myers & Sundaram, 2013; Misoch, 2015).

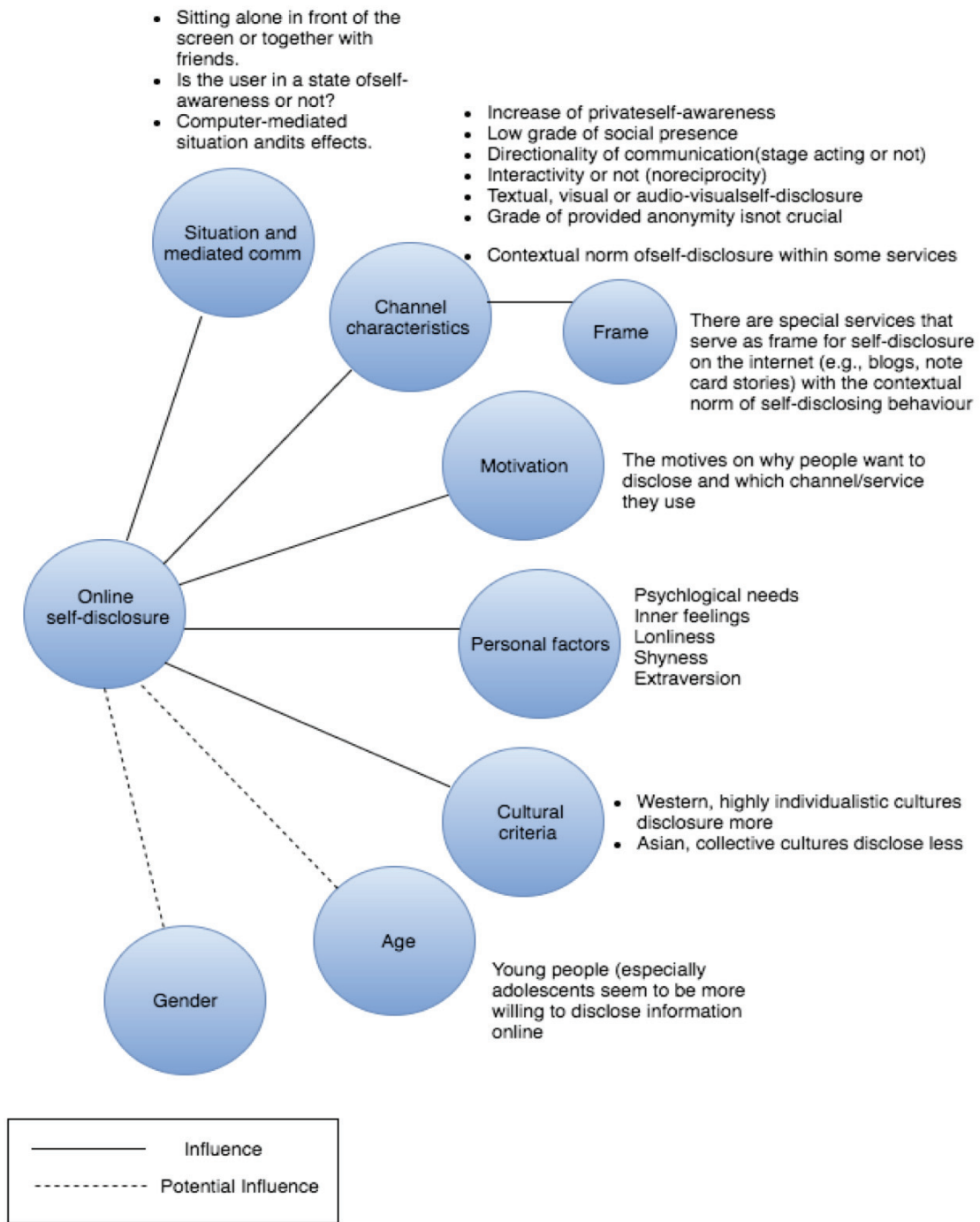


Figure 2.3 Factors that influence self-disclosure. Modified from (Misoch, 2015)



### 2.2.3 Privacy Awareness Support

In Chapter 1, we adopted the meaning of privacy awareness according to Pötzsch (2008) work as “the attention, perception and cognition of”:

- Whether others accessed or have accessed personal information about the user, his/her activities or presence.
- What information they accessed or have accessed in detail.
- How this information has been processed or used.
- What the amount of information about the presence of others and their activities reach to the user and/or interrupt him/her. (Pötzsch, 2008)

Privacy awareness stimulus is represented with content and representation of information. These content and representation differ based on two parameters. The parameters are the user and the application. Table 2.1 shows the values for each parameter (Pötzsch, 2008).

Table 2.1 Dimensions of Privacy-Awareness Information. Table from (Pötzsch, 2008)

	User-independent	User-specific
Application-independent	Talks, Campaigns, Tutorials	Individual advice from a Privacy Commissioner
Application-specific	Privacy Disclaimers on Websites	Feedback from Website’s Policy evaluation (e.g., Privacy Bird)

Table 2.1 shows examples of each dimension. When building privacy awareness information, *user-specific* means that the stimulus is tailored to each user of a system or a specific group of users or it is built according to user needs. *User-independent* means privacy awareness information is a hint for any user in general, such as Privacy Disclaimers on Websites. Whereas Application-specific means the stimuli is built for a specific application, and Application-independent is “independent from any special use case” (Pötzsch, 2008).

The tools that support privacy awareness of people serve as reminders about the passive users who the user unaware of their presence. The ultimate goal of the privacy awareness is to mitigate unwanted and uninformed privacy violation. There are requirements to build these tools; we list them briefly bellow (Pötzsch, 2008).

- Measuring user privacy attitude, so that the tool supports the intended purpose.
- The tool should not interrupt or annoy the primary user task.
- The tool should convey the message and be designed in an understandable manner for non-expert or non-computer specialists to have a usable application (Adams & Sasse, 2001; Pötzsch, 2008).
- Considering the mental model of a user, meaning that the tool should be able to handle the privacy awareness information cognitively.
- The tool should be designed based on a specific situation or context, i.e., “the task, kind of information, recipients, usage, etc.”. Therefore, it needs to be user-specific and application-specific.
- The tool should be seen as a supporter of privacy awareness, not fully responsible for protecting one’s privacy.
- The tool should not negatively affect the performance of the primary application to some extent. (Pötzsch, 2008).

In the next section, we explore the area where we can apply privacy awareness tools and mechanisms for live video broadcasting.

## **2.3 Privacy Issues Associated with Live Video Broadcasting**

Two of the major privacy issues associated with live video broadcasting concern the protection of location data and the maintenance of visual privacy. Each of these issues is discussed in detail below.

### 2.3.1 Location Information

Thomas, Briggs and Little (2013) adopted a theoretical psychological framework of location-based services (LBS) with the aim of predicting users' intentions to employ LBS in the context of social networks. There is a general trend of people not hesitating to share location information in this case, due to a perceived trust of social networking sites and a lack of concern about their intentions (Thomas et al., 2013; Beldad & Kusumadewi, 2015). According to the Unified Theory of Acceptance and Use of Technology, users accept or refuse a technology depending on the perceived ease of use and benefits that can be obtained from the technology (Widjaja et al., 2012; Beldad & Kusumadewi, 2015). Moreover, the Uses and Gratification theory indicates that a user tends to use a technology if it satisfies social and psychological needs in terms of entertainment, information seeking, personal identity or social interaction (Beldad & Kusumadewi, 2015). In addition, according to a study conducted specifically on location sharing applications, social influence, which reflects the degree to which others have influence on an individual in terms of trying a new system, affects user decision to adopt location-sharing applications (Widjaja et al., 2012; Beldad & Kusumadewi, 2015).

One of the central privacy issues with live video broadcasting apps (e.g., Periscope) relates to its ability to show users' locations. According to location-sharing apps analysis, typically the main objectives of these apps (e.g., Foursquare, Glympse) are to track people, look for local places, tag speed traps, share trips and engage in location-based dating (Tsai et al., 2010). However, when a mobile phone has its location turned on, social networks (e.g., Facebook, Instagram) (Albrecht & McIntyre, 2015), including live video streaming apps that provide this feature (e.g., Periscope), can access the GPS coordinates that indicate the user's location and use that information for their services (e.g., linking or tagging a post, picture, or video with its location of origin) (Albrecht & McIntyre, 2015). While this contributes to the functionality of such apps, it also means that travel plans or sensitive location information can be identified (Albrecht & McIntyre, 2015), creating an opportunity for thieves or malicious individuals to commit acts that include stalking, which may become particularly easy if precise location is available (as with an app such as Periscope). In the case of live video apps (e.g., Periscope), where showing faces (someone's identity) and locations are critical to using the platform, privacy risks may be outweighed by the benefits, or simply by the functional necessity,

of providing such information. Therefore, there is a need to further investigate the reasons behind showing the precise location to the public from a user perspective, so that solutions can be addressed according to users' understanding and needs.

### *Anonymity and Obfuscation*

Privacy protection methods related to location information have been addressed; they include anonymity and obfuscation. In this context, *anonymity* means a disconnection between an individual's information (e.g., location) and the individual's actual identity (Duckham & Kulik, 2006). Spatial Cloaking is a mechanism within anonymity that provides an individual's location based on "the number of other individuals within the same quadrant" (Duckham & Kulik, 2006). Anonymity sometimes constitutes an obstacle for authentication because it does not disclose identity information to a third party, which is required for some applications. Pseudonymity is a special variety of anonymity "where an individual is anonymous, but maintains a persistent identity" (Duckham & Kulik, 2006; Krumm, 2009). Meaning that users can replace their identity with a pseudonym that conceals their real identity. Obfuscation is "the process of degrading the quality of information about a person's location," with the objective of protecting location privacy (Duckham & Kulik, 2006). Obfuscation may take three forms: inaccuracy, imprecision and vagueness (Duckham & Kulik, 2006). Inaccuracy means that the location information being shown is totally different from the actual location information. With imprecision, information about the region containing the actual location is available (e.g., the city), but not the precise location itself (Krumm, 2009). Vagueness refers to a linguistic description of how far person A from a specific location (Duckham & Kulik, 2006).

In this research, we used vagueness, which is similar to the above techniques, to view the location of viewers to the broadcaster. The reason for using vagueness as a feedback method about viewers is that we want to protect the viewers' privacy as well. According to Jedrzejczyk (2012), who suggested design guidelines for feedback mechanisms, the information of others on real-time feedback should not be disclosed in details to reduce intrusiveness as well as their privacy might be affected. We applied this by describing to the broadcaster how close or far the location's viewers are from the broadcaster's location.

## *Feedback Mechanisms*

In the context of privacy and self-disclosure, feedback is defined as “informing people when and what information about them is being captured and to whom the information is being made available” (Bellotti & Sellen, 1993; Jedrzejczyk et al., 2010). The effectiveness of feedback in terms of mitigating privacy concerns has been demonstrated by numerous studies. One study proposed a method to nudge the user, through permission manager, about applications that access the user’s sensitive information. The results showed that the method prompted users to place restrictions on some applications that do not necessarily need to have access to their personal information, including location (Almuhimedi et al., 2015), suggesting that such privacy nudges help users to make decisions about their privacy (Acquisti, 2009) (Almuhimedi et al., 2015). At users level, receiving feedback about users who viewed one’s location made the user less concerned about sharing location (Tsai et al., 2009).

Jedrzejczyk et al. (2010) classified feedback into three dimensions: “sensory”, “interaction” and “time”. The sensory dimension includes auditory, visual and tactile feedback. The interaction dimension may be either automatic (e.g., feedback is given automatically when someone requests one’s location) or on demand (e.g., a user shakes his phone to display who requested his location). The time dimension signifies the provision of either real-time feedback, which supports awareness, or aggregated feedback in the form of a log detailing instances of information access. Some examples of feedback mechanisms are discussed below.

In one example, LED light was used as a form of feedback in *RAVE* (Remotely Accessible Virtualized Environment, a virtual system that allows different users to exchange information using various multimedia including video, audio, and 3D (Jedrzejczyk et al., 2010). The purpose of LED light usage is to display information about when people were being recorded. This worked well as feedback but proved distracting when large numbers of people were being recorded (Gaver, 1991; Bellotti & Sellen, 1993).

Hong and Landay (2004) proposed a “Just in time” description of who requested information and why, as displayed in a dialog window that provides three options (“Accept”, “Ignore” and “Deny”) so that the user can make informed decisions regarding whether or not to share information (Hong & Landay, 2004; Jedrzejczyk et al., 2010). While this approach is promising, the use of a dialog box during live video broadcasting can be disruptive.

In another case, Bellotti and Sellen (1993) used auditory cues for software simulation,

playing audio cues to provide feedback and support (e.g., a voice tape as a guidance of how things work) in the context of collaborative workstations. However, using auditory feedback in contexts other than collaborative environments (i.e., in public) could be annoying, embarrassing or distracting for users.

Prabaker et al. (2007) designed a real-time feedback system using bubble notifications for the PeopleFinder application, which allows one to selectively share his or her location with others (see Figure 2.4). The feedback provides details on any request of the user's location, in accordance with the privacy policy. If the user does not set his location privacy policy to be viewed to others, no one can request his location. The researchers also proposed aggregated feedback as a historical list of people who requested the location. Although the findings were positive with respect to people who felt comfortable sharing their location, bubble notifications were deemed distracting. It was also suggested that systems should make the users feel comfort with their ability to control their own privacy policies over time (Prabaker et al., 2007).

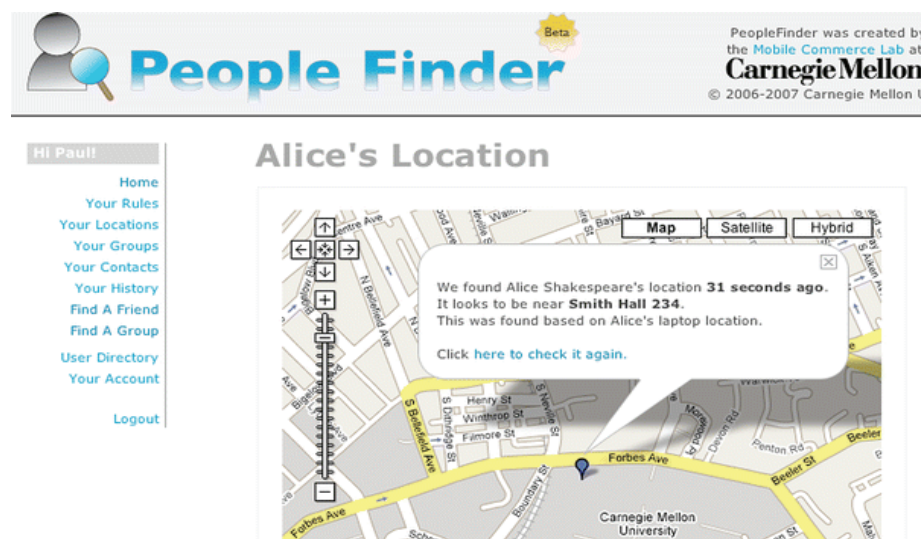


Figure 2.4 A screen capture of People Finder App. Figure from (Sadeh et al., 2009)

Jedrzejczyk et al., (2010) presented a similar feedback system for the sharing-location application Buddy Tracker that includes real time and aggregated feedback. The real-time feedback system proposed here is based on the concept of social translucence, and aims to provide three things: awareness, visibility, and accountability (see Figure 2.5). The feedback informs the user about who has requested his or her location among the group of users listed in the application, in accordance with the user's privacy settings. In this system, real-time feedback

was provided in the form of an SMS sent directly to the user. Users found the SMS feedback disruptive in the contexts of work, online chatting, or playing online games. Even though findings indicate that users were being held accountable for requesting each other's location, feedback would be excessively intrusive in the context of a large number of viewers. Real-time feedback needs to be further explored with the aim of being non-intrusive and affordable, such that it can accommodate many viewers.

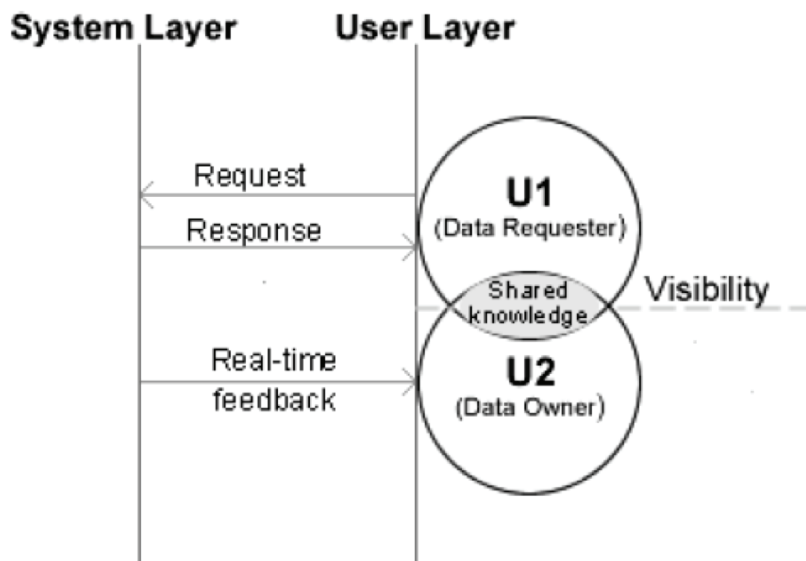


Figure 2.5 Social translucence for Buddy Tracker. Figure from (Jedrzejczyk, 2012)

Jedrzejczyk (2012), in his later work proposed context-awareness real-time feedback to solve this problem. Context-awareness real-time feedback means that the app is able to sense the user's environment, through sensors and with the support of incremental learning algorithms, so that provides an appropriate privacy preference to the given context (e.g., hide/blur location based on specified people or for specific time).

The functionality of this kind of feedback is to provide an explanation of the context to the user, and then to ask the user about his or her feedback regarding the accuracy of the information presented. Jedrzejczyk (2012) implemented context-awareness real time feedback that relied on users' answers to a predefined questionnaire. The questionnaire concerned how information of someone checked the user's location should be conveyed (e.g., sound, flashing lights, notification bar). In particular, when the action of requesting a user's location occurs, the

app provides notification, and 5 minutes later, an SMS is sent to the user containing a link to a questionnaire asking whether the accuracy of the event context is accurate and whether the feedback representation is appropriate for that context; it also asks the user to suggest which feedback is most appropriate for informing the user about in a given context. However, users did not notice improvement in system accuracy. The weaknesses of this method include possible shortcomings in information accuracy and the substantial user effort required in answering questions about the feedback. Thus, it may not represent the most efficient approach; especially if we consider the context of live video broadcasting.

Gaver (1991) proposed the use of privacy birds as a way of comparing a given website's privacy policies with the user's privacy preferences. These privacy birds could be green, red and yellow, indicating different degrees of matching, with an option of also playing sounds. Despite the fact that this type of feedback can save the user from having to read the long textual privacy policies, users sometimes misinterpreted the bird icons with respect to websites' safety setting. This occurred partly because some of the icons are ambiguous and not obviously tied to their own meaning; for example, a happy singing bird was interpreted by users as playing music or an angry bird as expressing bad language. As design criteria, icons should carry obvious meaning; one way to do that is using internationally recognizable icons, so that there can be no doubt regarding the symbol's information content.

To our knowledge, all feedback systems associated with location requests have been designed for identifying identified users within the given app, but do not provide information on strangers (i.e., non-defined users of that app, who are not among the users' contacts). Furthermore, feedback typically applies to those who have explicitly requested location information, but not to those who have automatically viewed that information. Considering these two issues, there may be a large pool of people receiving users' location information without those users being made aware. Moreover, previous studies proposed feedback presenting static information about the viewers, rather than dynamic information; that is, the location information in most cases represents the location only at a single moment and fails to continue tracking.

In this study, we propose a part of a privacy management system that addresses some of the shortcomings described above. Specifically, we propose a static and dynamic real-time feedback system designed for someone who directly views someone's location without requesting it. Thus, the user is made aware of the overlooked segment of people who have not



gone out of their way to request such information, but have nonetheless accessed it. In addition, we explore the possibility of notifying or warning the user in the context of live video broadcasting to the public, with emphasis on establishing feedback that is not disruptive to the broadcasting process.

In order to build a dynamic real-time feedback about viewers who are moving in and out from the broadcaster's location, several main techniques are required. GPS is the most accurate positioning system that can be used to determine the viewer's location (Tsai et al., 2010). Google Geo service can then be used to translate GPS information into textual description (Jedrzejczyk, 2012). Shyhook's Core Engine SDK, fulfills location requests and produces accurate locations quickly, can also be used to determine the current position of the viewer (Jedrzejczyk, 2012). Different types of accelerometers can be combined to measure viewers' movement. Accelerometer is a "device that converts" either dynamic or static "acceleration into an electrical signal" (Naghshineh, Ameri & Zereshki, 2009). Dynamic acceleration is due to any force except for gravitational force, and the static is due to the gravitational force (Naghshineh et al., 2009). Naghshineh et al. (2009) presented the theories of accelerometers that capture human motions. We mention here some of them that can be used to implement our proposal in the future. Tri-Axis Tilt Sensing uses x, y, and z axes to sense tilt; compass sensors to measure direction; gyroscope used to measure how quickly an object turns (Naghshineh et al., 2009).

### **2.3.2 Visual Privacy Protection**

A recent form of online self-disclosure has emerged on YouTube in the form of "note card stories," characterized by having the presenter sitting in front of the camera, showing his face (or, sometimes, showing parts of his body but not his face), turning music on as background with no talking, and silently displaying his/her story written on cards (Misoch, 2014). According to 25 videos selected for analysis in (Misoch, 2014), 21 out of 25 publishers show their faces in these videos without being visually anonymized, and are therefore identifiable (Misoch, 2014). The common topics of these stories are "depression, suicidal thoughts, death of a parent or beloved ones... self-injury, eating disorders, divorce of parents, transsexualism, ..., alcoholism, panic attacks, rape, shyness, fears, religion, and loneliness." (Misoch, 2014). From this phenomenon, a principal issue arises that is related to the act of disclosing too much private information (e.g.,

their true, sad stories) while in a negative state, with no visual anonymity, which makes them vulnerable to strangers or untrustworthy people (Petronio, 2012; Misoch, 2014). Studies showed that the level of disclosure of information becomes higher in the case of computer-mediated communication than face-to-face communication (Misoch, 2014). What has been occurred on YouTube (e.g., Card Stories phenomenon) is likely to occur on live video streaming as well. Knowing that many users of this phenomenon intend to not show their faces while they are practicing it provides insight into the need for visual privacy protection.

In the context of live video broadcasting, facial recognition systems can collect the identity of a person, along with specific, sensitive information about that individual (Goessl, 2012; Padilla-López, Chaaoui & Flórez-Revuelta, 2015). Due to the tremendous amount of potentially sensitive information that videos can reveal, researchers have proposed techniques to preserve users' privacy. Techniques that are applied to video surveillance systems in order to protect the appearance of people who are not meant to be recorded are based on detecting sensitive information or the targeted area (Schaar, 2010), which is accomplished using computer vision algorithms (Padilla-López et al., 2015). Padilla-Lopez et al. (2015) classified a number of different visual protection techniques. The most appropriate and common method for the context of live video broadcasting is reduction, which involves modifying the sensitive area (e.g., face, body) to conceal private information of the subject (Padilla-López et al., 2015). Reduction techniques include image filtering (e.g., blur, pixelating to make the region of interest unrecognizable) (Zhang, Rui & He, 2006; Frome et al., 2009; Agrawal & Narayanan, 2011; Padilla-López et al., 2015), blurring (shifting pixels within an image in order to obscure details), and pixelating (averaging the colors of blocks of pixels in order to obscure information (see Figure 2.6). Another techniques include video encryption (e.g., the image is encrypted by a key using encryption methods), face de-identification (extracting and showing the facial expression, but not the actual face), visual abstraction/object replacement (replaces an object with abstraction, but not necessarily removing it), object/people removal or in-painting using in-painting-based algorithm (the object or people can be removed from the image by filling in the gap with the same background of that image) (Abraham, Prabhavathy & Shree, 2012; Padilla-López et al., 2015). They also suggested using in-painting in videoconference to remove “inactive participants from the video stream”. In addition, lightweight encryption is used for real time applications, which aims for reliable secure storage and secure transmission over network

(see Figure 2.7) (Padilla-López et al., 2015).

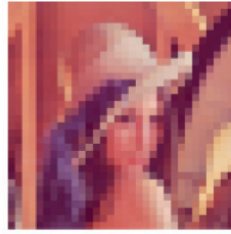


Figure 2.6 Pixelating: A visual privacy protection method. Figure from (Padilla-López et al., 2015)



Figure 2.7 An example of an encrypted image where the face of the person is considered the sensitive region. Figure from (Padilla-López et al., 2015)

Among these approaches, the ones that are applicable for real-time video applications, image filtering (e.g., blurring), in-painting, lightweight encryption and the scrambling technique, which involves making the content of an analogue video signal, and any resulting image, unintelligible. However, lightweight and scrambling techniques are encryption-based methods and are time consuming, though not as time consuming as naïve encryption.

Although other technologies (e.g., encryption-based methods) are more secure, they are not practical or efficient because they are time consuming in the context of live video. Thus, there is a trade off between security and encryption speed. As our research takes place at a relatively early stage of privacy in live video broadcasting, we need to know how the concept of visual protection technology is acceptable by the users. Therefore, we want to explore whether blurring or in-painting are acceptable.

To summarize, to build our survey, we drew upon existing theories related to user personality, usage of video-based social media, and also factors that affect self-disclosure. We also explored temporal live video broadcasting apps so as to fully understand their privacy attributes. To further this understanding, we also observed Periscope live video broadcasts over a period of one month, uncovering specific scenarios that warrant special attention with respect to privacy concerns; for example, we found that broadcasters commonly show their location to viewers, despite the risks associated with such behavior. For this reason, one aspect that we investigated in our online survey is how people perceive showing location to the public, and whether they consider privacy in the context of broadcasting. Another common observation was that broadcasters engage in self-disclosure and inappropriate behavior that raise privacy concerns and issues; most commonly, this involved broadcasting while under the influence of alcohol. The type of descriptive statistics about recent temporal live video broadcasting apps that we aimed to collect in the survey are critically necessary to understanding the relationship between numerous factors and drawing conclusions about the kinds of privacy features that can be embedded in these kinds of apps in order to preserve user privacy.

Our second study was a design exploration of ways to detect and address privacy concerns commonly associated with using these apps. We adopted the concept of Real-time Feedback mechanisms from previous studies in order to propose a dynamic awareness-based solution for notifying the broadcaster about viewers who automatically view the broadcaster's location without request. The mechanisms also provide more detailed information about the movement of those viewers, including strangers, when they are getting around the broadcaster's location. We also adopted visual privacy protection methods (e.g., blurring and in-painting) in order to design mood-based visual privacy awareness mechanisms. Since the literature shows that many social media users are extroverted and emotionally unstable, the proposed mechanism was designed to protect those who broadcast live videos in altered states, whether related to mood or to substance intake.

## **CHAPTER 3 USE AND PRIVACY PERCEPTION EXPLORATION**

In this chapter, we explore people's perception toward the use and privacy of live video broadcasting apps. We first describe our survey methodology, and our targeting participants. Then, we describe the study procedure, outlining the research questions to address in the survey, and how we designed our online survey based on usage and privacy measures. We then present and discuss the results of the survey, and finally point to the limitations, highlighting future directions of the survey that can be used to develop the survey.

### **3.1 General Approach and Methods**

A number of studies have examined issues related to privacy in social media and its social interactions, especially in relation to videos. However, research in this rapidly developing area of technology is lacking with respect to privacy issues related to newer forms of social media, including temporal social media and, in particular, live video-based broadcasting applications.

Therefore, the first phase of this research was an exploration of the relationships between various variables. We surveyed live video app users to address the patterns of, and reasons for, the use of these apps by broadcasters, i.e., those who have created videos, and therefore excluded app users who have only viewed such videos. The survey also addressed the perceptions and use of privacy and security issues for broadcasters.

We specifically targeted users of YouNow, Meerkat and Periscope, although we did not limit participation to those apps (if there should be other apps). Periscope has unique privacy concerns due to its features, which include allowing the video to be saved temporarily and allowing the location (in GPS) of the broadcaster to be shown by default. Therefore, we devoted a portion of the survey specifically to Periscope.

### **3.1.1 Participant Recruitment**

We recruited participants who use any live video broadcasting social app, including but not limited to Meerkat, Periscope, or YouNow. Broadcasters could be located anywhere in the world; indeed, because it has been found that culture has implications on privacy conception (Acquisti et al., 2015), we wanted a representative sample of the international population. That is, one should consider the implications of culture on the privacy and use of these modern mobile apps (the temporal/self-destructing live video broadcasting apps).

To recruit the participants, we posted notices on Twitter, Facebook, Google+, and Instagram using hashtags #YouNow, #Meerkat and #Periscope and other relevant hashtags (See Appendix A). We recruited those who use these apps only for creating broadcasts, and excluded those who only view broadcasts created by others. In addition to recruiting internationally using the apps themselves, we recruited from the local community using the Dalhousie University Computer Science mailing list. This mailing list included the faculty, staff and students of the Faculty of Computer Science. The online recruitment and survey was completely anonymous. This anonymity can provide potential participants a sense of privacy that is not available in a face-to-face interaction (Rudestam & Newton, 2007, p. 92).

### **3.1.2 Study Procedure**

Participants were fully informed and provided explicit consent. The recruitment materials (See Appendix B) provided a link to the survey on the Dalhousie Opinion Survey Software system. When participants went to the opinion website, they were presented with a short summary that provided general information including the notions that participation is voluntary and that data collection is anonymous. At this point, potential participants were provided with the opportunity to ask questions through e-mail contact. If still interested, the potential participant continued to the informed consent.

The second page was the informed consent, which included the study goals, data to be collected and the option to consent. The consent form explicitly stated that participation is voluntary, that the participant can withdraw at any time without penalty, that the participant can choose to not answer particular questions if he or she is unwilling to answer, and that the

collected data is anonymous. The informed consent described the purpose of the study and the inclusion/exclusion criteria and listed the demographic (background) and study data to be collected. It then described the risks and benefits associated with the study.

The consent form in the website ended with a two-button option: One option to continue onto the survey and the other to exit the process.

### **3.1.3 Research Questions**

The online survey was organized into groups of questions that were designed to answer specific questions regarding the use of live video broadcasting apps, as well as issues related to privacy and self-disclosure. The survey questions, along with notes on their development, can be seen in Appendix C.

The first block of questions addressed the demographic characteristics of those using the apps, as well as why and how they use them. These questions also asked users whether or not they considered privacy concerns in choosing to use the apps. The next block of questions examined users' awareness of privacy issues related to the temporary nature of these apps' videos, user concerns related to that topic, and what aspects of privacy they would like to see improved. The questions that followed asked users about the benefits and risks of two specific features of the Periscope app: its retention of videos and its display of broadcaster location.

Subsequent questions looked for connections between users' privacy concerns and various aspects of video broadcasting apps. These factors included characteristics of the users, including demographics and knowledge of computer security, and elements of how the apps are used, including types of broadcasts and reasons for doing them. Lastly, the survey asked users about the relationship between the relationship between the positive and negative aspects of the temporary nature of broadcasts.

### **3.1.4 Study Instrument and Measures**

The instrument used in this stage of the research was online survey. We chose to conduct an online survey because it enabled us to gather data from a large number of participants, which was necessary due to the lack of basic information about use of these apps. For that survey, we

used *closed-ended questions* (questions that require the participant to select an answer from a group of given possible answers (McIntyre, 1999, p. 75)) because they can be analyzed quantitatively and are therefore more suitable for large samples. In particular, we used a mix of *ordered items* (items that ask the participant to select a response using a numerical or Likert scale; this also includes binary responses of the type Yes/No, Agree/Disagree, or similar) and *unordered items* (ask the participant to select one of several options using nominal scale. That is, the options are not ranked by degree; they are merely different. This is classically used in multiple choice tests), and a few items allowed for the participant to provide a response.

The online survey was divided into three sections: The first section collected demographic and background information. The second section collected information about the use, privacy perceptions, self-disclosure behavior and user privacy preferences for live video broadcasting apps. The third section collected information from participants who use the Periscope app (see Appendix C).

## ***Measures***

In the first section, seven questions were used to collect basic demographic information about the participants. Since individuals differ with respect to factors related to both demographics to personality, these questions are necessary in order to understand user traits (see Appendix C). The following are the measures we used to investigate the use and privacy.

### ***1. Usage***

Questions 8 to 15, we asked how and why live video broadcasting apps are used, with particular interest in whether such aspects of usage are associated with concerns and behavior related privacy. We used operational definitions for usage that include frequency of use, how often specific behaviors occur, frequency of an activity, continuous self-report questions (e.g., place of that use and associated emotions), and self-perception attitude about frequency of use.

### ***2. Knowledge About Temporal/“Self-Destructing” Nature of Live Videos Broadcasting Apps***

Since we are interested more in “Self-Destructing” and temporal live video broadcasting apps, we examined participants’ knowledge about the availability of the broadcasts in questions 16 and 17.



### ***3. User Perception toward Temporal/“Self-Destructing” Nature of Live Video Broadcasting Apps***

To better understand how people think about the temporary nature of live video broadcasting apps, including the possible influence of privacy concerns, we explored the advantages and disadvantages of these apps in two independent questions, 18 and 19. One explores why users might see the temporary nature of the videos as a positive feature of the app; the other asks why they might see this feature as a negative aspect.

### ***4. Privacy Perception according to Privacy Preferences***

In Question 20, we intended to investigate what kind of privacy control users want and need for live video broadcasting apps. Since user personality has effects on self-disclosure behavior and privacy preferences, we asked about their privacy preferences toward specific sensitive information (See Appendix A). In questions 21- 23, we aimed to examine privacy features related to face, voice and location, respectively, by exploring participants’ knowledge of potential risks associated with showing the three features, which are parts of their identities, while broadcasting.

### ***5. Privacy Perception According Privacy Concerns***

We asked participants about the level of their concerns in Question 22.

### ***6. Privacy Perception According Privacy Awareness:***

The primary social interaction that occurs during live video broadcasting is between the broadcaster and the viewers. As one objective of this research is making the broadcaster aware of his/her privacy, in Question 23 we asked participants what privacy control and/or awareness about viewers they would like to have.

### ***Periscope Section***

Only Periscope users were directed to the third section, “Periscope Users”. Since we are using Periscope as an example for designing our proposal in the next phase.

### ***Privacy Practice/Privacy Attitude:***

We asked Periscope users a number of questions in order to classify them into one of three groups with respect to their attitudes towards privacy concerns: fundamentalist (high concern), pragmatist (medium concern), and unconcerned (low concerns) (Madejski et al., 2011).

### **3.1.5 Analytic Plan and General Comments on Issues for Statistical Analyses**

In the next section we present the results in 6 sections: These sections include the Apps Used, Reasons for Use, Categories of Use, Concerns and Issues for Use, Periscope Use, and Relationships between Variables. All analysis was conducted in SPSS with the assistance of a professional statistician, B. W. Frankland, PhD, P-Stat (Canadian Statistical Society), who helped writing this section.

The first four (Apps Used, Reasons for Use, Categories of Use, Concerns and Issues for Use) are the basic questionnaire. We only present basic descriptive (summary) statistics. This basic questionnaire is one of our main contributions to the literature. It tells us how the apps are being used and what concerns broadcasters have for those apps.

The next section is the part of the questionnaire about Periscope. Again, we only present descriptive statistics about use. This is also part of our main contribution to the literature because the information is not known and Periscope is the most commonly used app possibly because of the extra features it offers.

The relationships between the variables section looks at how the results Apps Used, Reasons for Use, Categories of Use, Concerns and Issues for Use and Periscope use are related to each other. For example, we looked at whether or not the people who used different apps had different concerns. Periscope has unique abilities so we thought that the people who use it might have unique concerns.

For Apps Used, Reasons for Use, Categories of Use, Concerns and Issues for Use and Periscope use, means and SDs have been presented. These are only used for variables that are continuous (like age or education). This includes variables that are rankings (like age and education). The other variables are dichotomies (variables for which there are only two possible answers as for example "yes" or "no"). These are also called binary variables. For the dichotomous variables, the percentage of people who "endorsed" the question is presented, the

number of people who said "yes" when asked about a particular thing. Percentages are presented, rather than actual sample sizes (e.g., 20.4% rather than 9 of 44) because percentages make more sense when trying to relate the data back to the population which is all broadcasters who use these apps.

We also examined the correlations between variables. These were conducted within sets of variables (e.g., within the set of variables for Apps Used). Correlations show the amount of association between variables — whether or not things go up and down together. As such correlations to clarify the interpretation of the set of variables, and they can help to simplify the set. If two variables in a set are highly associated, then only one is needed (the other is “extra” or “redundant”). The simple Pearson correlation is used for all correlations ( $r$ ).

As noted above, some of the variables are dichotomies (binary). The Phi-coefficient ( $\Phi$ ) is often used when looking at the relationships between two dichotomous (binary) variables. However, as noted by Howell (1997, p. 283) the computations for the Phi ( $\Phi$ ) and the Pearson ( $r$ ) are algebraically identical. At other times, the Pearson chi-square test ( $\chi^2$ : usually called the chi-square) is often used with dichotomous variables, but the chi-square is just a linear transform of the Phi (i.e.,  $\Phi = \sqrt{\chi^2/N}$ ); see Howell, 1997, p. 158, 284-284). Howell stated “It should be apparent that in calculating  $\Phi$  and  $\chi^2$ , we have been asking the same question in two different ways. Not surprisingly, we have come to the same conclusion” (p. 285). The Phi ( $\Phi$ ) is the same as the Pearson ( $r$ ). In principle, there is a slight difference between the Phi and Pearson. The  $\Phi$  is typically tested against the chi-square distribution while the  $r$  is tested against the t-distribution. However, the results rarely differ (we will provide some examples in the first few analyses; see the analysis associated with Table 3.4) because there are strong theoretical links between the two distributions (see Howell, p. 135 - 137). In addition, we must be careful about the interpretation because the binary variable can represent a true dichotomy (e.g., in “I own the Periscope app?: Yes/No”; Male vs Female) or a continuum (e.g., “I use these apps when happy: Yes/No”). There is an implied continuum for the happy dichotomy (i.e., degrees of happiness) that the only approximated by the binary code. There is no continuum for ownership: Either you own it or your don't. There is no continuum for gender. Howell (p. 286) also points out that small values of  $\Phi$  can be important.

When one variable is a dichotomy and the other variable is a continuum (e.g., the relationship between gender and education level), the point-biserial correlation is often used. The

point-biserial is identical with the Pearson correlation (Howell, 1997, p. 279-281). In fact, the point-biserial correlation is the same as a two-group t-test (Howell, p. 282-293) when the dichotomy is used to define the groups as the independent variable or IV. The continuous variable is the dependent variable or DV. Hence, we have used the Pearson correlation.

The interpretation of correlations was based on the size of the correlation and not on the statistical significance. The correlation-squared is a standard measure of effect size (see Howell, 1997, p. 247-251). A correlation of  $r = 0$  between two variables (e.g., Variable A and B) implies complete independence (this is also called orthogonality). The two variables are unique; they have nothing in common. A correlation of  $r = 1$  (or  $r = -1$ ) implies complete dependence. The two variables are really the same (i.e., “identity”). They are two names for the same one thing. Values between 0 and 1 (or between 0 and  $-1$ ) imply some independence and some dependence. A low correlation (near 0) implies that they are more independent than dependent: Each is basically unique. A high correlation (near 1 or  $-1$ ) implies that they are more dependent than independent. They are almost the same as one variable with two different names. The difficulty with the interpretation of correlations is deciding what is “high” and what is “low”: There are no rules, but there are some guidelines.

It is the correlation-squared ( $r^2$ ) that actually defines the overlap between variables (often called the “proportion — or percentage — of variance in common”). In this thesis, we are using a simple guideline for the size of a correlation. A correlation-squared ( $r^2$ ) that is less than 0.10 is called “small”. If  $r^2$  is less than 0.10 (i.e.,  $r^2 < 0.10$ ), then the absolute value of  $r$  is less than 0.316 (i.e.,  $|r| < 0.316$ ). A correlation-squared ( $r^2$ ) that is between 0.1 and 0.5 is called “moderate” (this implies that  $0.316 < |r| < 0.707$ ). A correlation-squared that is above 0.5 is called “large” (this implies that  $|r| > 0.707$ ). We are using these guidelines for this work, but we acknowledge that these are just guidelines and there are others. For example, in the context of a two-group t-test, Cohen (1988, p. 25) defined effects sizes of less than 0.2 as small, 0.2 to 0.8 as medium (i.e., around 0.5), and greater than 0.8 as large. These correspond to  $r < 0.100$ ,  $0.100 < r < 0.371$ , and  $r > 0.371$ ). Our definition of a small correlation implies that Variable A is one of 10 (or more) equally strong (independent) variables that explain Variable B (i.e., Variable A explains less than 10% of Variable B). It is possible that there are other stronger variables. Our definition of a moderate correlation implies that Variable A is one of between 2 to 9 (independent) variables that could explain Variable B — that is, there could be 9 other equally

strong variables, or there could be a few stronger variables. Our definition of a strong correlation implies that there are no other (independent) variables that explain more than Variable A.

In the complex real world, it is possible for a single variable to correlated with “many” other variables, but for all those correlations to be in the small range. This is the type of situation that would be expected for our study. For example, the decision to create a single BC may be “caused” by 20 or 30 other factors such as interest, time, potential rewards (which might includes money, prestige, feels of self worth, even guilt), available equipment, potential viewers, personal privacy risk, privacy risks for others, and security risks (which might include lawsuits, employer monitoring). As such, we feel that we should *not* ignore small correlations just because they are small. In addition, all of these other factors may be related to (correlated with) each other. For example, rewards might be related to viewers. There is a correlation matrix for all the variables of current focus. Surveys are hard to interpret because there may be many relationships (the correlation matrix) and all the relationships may be small. In this thesis, we have tried to present the correlations in understandable sets. Simplistically, it is the pattern within each set that matters (not the individual correlations in isolation), and the patterns between sets. For sets of variables, the mean correlation are provided because it indicates the average association within a set, the range of correlations (maximum degree of association), and the average of the absolute values of the correlations because the simple mean might be artificially low when the matrix contains a mix of negative and positive correlations (i.e., there could be 5 high positive correlations and 5 high negative correlations, which would have a mean near zero, but this under-represents the amount of relationship).

In the analysis of correlations, significance is less important. A significant correlation implies that we can be reasonably sure that the *true* correlation in the population of all app users is *not zero*. This is useful because it implies that there truly is some kind of a relationship *in the population*. However, significance itself does *not* provide any indication of size or strength of the relationship. Significance only implies that the true correlation in the population is “not zero”: it could be “not zero” and yet still small. Regardless of significance, the correlation observed in this sample is still the “best guess” (best estimate) of the true correlation in the population of all app users.

Sometimes we want to look at the differences between the means of groups (e.g., the mean difference on educational level for males vs females). If there are only two groups, this can

be done with a t-test. If there are more than two groups, we use an ANOVA. The ANOVA is just the extension of the t-test to compare more groups. In fact, the ANOVA can be used when there are just two groups (the two-group ANOVA is identical with two-group t-test). There are two types of ANOVA. The between-subjects ANOVA is used when each group contains *different* people. This is used when, for example, we want to compare men vs women on some variable. The within-subjects ANOVA is used when all groups contain the *same* people who have been measured more than once. This is used when, for example, the same group of people have been measured on their tendency to BC at home and their tendency to BC at work (to see if location matters). The within-subjects ANOVA is also called the repeated measures ANOVA because it represents repeated measurements on the same people. The within-subject ANOVA assumes that the variables involved are correlated (e.g., tendency to BC at home would be correlated with the tendency to BC at work). It is also called the dependent measures ANOVA because variables that are correlated are “dependent” to some degree. It is also called the correlated samples ANOVA though this is not common outside theoretical statistics. Finally, there is a within-subjects version of the t-test that is mathematically identical to the within-subjects ANOVA with two variables. It is called the dependent samples t-test, paired t-test or correlated samples t-test.

As noted above, some variables are ordinal scales. These will be analyzed using the between-subjects or within-subjects ANOVA where appropriate. Some people argue that we should use “distribution free tests” (a.k.a. non-parametric tests). The distribution free analogue of the between subjects ANOVA is the Kruskal-Wallis ANOVA of Ranks. The distribution free analogue of the within-subjects ANOVA is the Friedman’s Rank test. These are not used herein for several reasons. As noted by Howell (1997, p. 645) writes “The argument over the value of distribution free tests has gone on for many years and it certainly cannot be resolved in this chapter. Many people believe that for most cases parametric test are sufficiently robust to make distribution free tests unnecessary. Other, however, believe just as strongly in the unsuitability of parametric tests. Herein, one main advantage of distribution free tests is irrelevant. Distribution free tests are less sensitive to “outliers” (extreme scores). However, in this questionnaire, all responses to the questionnaire were constrained (i.e., people could only select from a limited number of options), outliers are not possible. Hence, distribution free tests were not used. In addition, distribution free tests tend to have lower power (Howell, p. 646), though usually the results are not sufficiently different to affect the decision to accept or reject (some examples will

be provided: see the analysis of data associated with Table 3.36).

Finally, there are times when we want to compare the percentages (e.g., percentage endorsement) for a dichotomy as a function of groups (the IV). If the DV is a true dichotomy (e.g., ownership as a function of gender), we use a Pearson chi-square. If the DV is a dichotomy that implies a continuum, we use an ANOVA. We could use a chi-square for this situation but an ANOVA for a DV that is a dichotomy is functionally equivalent to (but not *identical* with) the chi-square. The p-values are very similar and the subsequent decisions about accept or reject are the same.

For the sixth section (Relationships between Variables), we only consider the more important relationships. We use the same analyses: correlations and ANOVAs.

Finally, in all analyses, the standard type 1 error rate of  $\alpha = 0.05$  (5%) is used. However, the exact p-value for each test is supplied in case the reader may want to apply a correction to the type 1 error rate. Coincidentally, for a sample size of 44 (the current sample), a correlation of  $r = 0.297$  is significantly different from 0 when using  $\alpha = 0.05$ . Hence, the previous guidelines delineating a small from a moderate correlation also delineates a significant from a non-significant correlation (approximately). That is, in the current work, a small correlation is not significant, whereas a moderate correlation is significant. Note that this coincidence is just an approximation because correlations near  $r = \pm 0.3$  need to be checked, and because sample sizes fluctuate a bit due to missing values. For example, if the sample size drops to 40, a value of  $r = 0.312$  is significant. As an aside, a correlation of  $r = 0.386$  ( $r = 0.401$ ) would be significant with a type 1 error rate of  $\alpha = 0.01$  for  $N=44$  (at  $N = 40$ ).

Note that all the tests used in this thesis are parametric. Many people categorize the chi-square as a non-parametric test, but this is misleading and incorrect (notably, the writer of the Wikipedia article on non-parametric tests does *not* classify the chi-square as non-parametric technique). A test is parametric if it uses a sample statistic (e.g., mean, correlation) to test an assumption about the value of a population parameter (e.g., the population mean, the population correlation). Note that testing a population parameter immediately presupposes an assumption about the population. The ANOVA is parametric because it tests the assumption that 2 or more *apparently different* sample means all could have come from one single population (with some unknown *single* population mean value). The t-test does the same for just 2 groups. The test of the correlation is parametric because it tests the assumption that the *apparently non-zero* sample

correlation could have come from a population with a correlation of zero. A population with a correlation of zero implies a complete lack of association between the two variables. Note that a dichotomy by dichotomy or a dichotomy by continuous can be (and is) analyzed as a correlation. The chi-square used is a bit more complicated, in part because many different tests are called a chi-square. The Pearson two-way chi-square used herein is a test of the association. It is equivalent to the phi-correlation. This chi-square test compares observed counts to expected counts, but the expected counts are based on the conditional probabilities. The conditional probabilities are based, in turn, on the marginal probabilities. The marginal probabilities are the probabilities for each level of each variable (e.g., in the case, the number who said “yes” or “no” for each of the two variables concerned). As such, the chi-square uses the marginal probabilities to create (more accurately: “to select”) the proper theoretical distribution for the expected counts (i.e., the conditional probabilities) *assuming* that there is no association between the two variables (i.e., this is the same as assuming the correlation is zero). It then uses the sample statistics (the observed counts) to determine whether or not the expected counts are correct. The expected counts are the parameters of a multinomial distribution (i.e., theoretical distribution). If the theory is wrong, there is an association between the two variables. Even the one-way chi-square is a test of the parameter  $p$  of the binomial distribution (typically, a test of  $p = 0.5$ ).

All tests require assumptions. Even non-parametric and distribution free tests have assumptions, though generally, the number and/or the specificity of the assumptions is less than those of the parametric case. These assumptions are often presented in different ways, and some writers skip some assumptions (presumably, they are “obvious”). All assumptions relate to the test of the null (or statistical) hypothesis — not the alternative (or research) hypothesis. The test is about rejecting or “accepting” (properly “failing to reject”) the null hypothesis. The alternative hypothesis is not involved except perhaps as vague considerations of power (see below). For the ANOVA (and t-test) the primary assumption is that each group is a single random sample (RS) from a single defined normal population with mean  $\mu$  and standard deviation  $\sigma$ . The assumption of a random sample is often denoted as the assumption of independent samples (or “independence”). The test compares the group means, and uses size of the differences between those means to reject (or “accept”) the assumption that all groups come from one population. The test assume that the standard deviations are the same in all groups (because all group are assumed to come from one population), and it uses this information as part of the test. This is



called the assumption of homogeneity of variance (a.k.a. homoscedasticity). The test also assumes that the variable being measured (the DV, not the IV) is a proper interval or ratio variable (i.e., a continuous variable). To the extent that these assumptions are not true, the result of the ANOVA is less reliable. However, the ANOVA is a robust technique. Numerous studies have shown that even large violations of the assumptions have little impact on the final p-value (i.e., the reported p-value is likely within  $\pm .02$  of the true p-value; see Howell, 1997, p. 340-342 for a review). Said another way, the final p-value for the ANOVA is particularly sensitive to difference between means, but relatively insensitive to other assumptions. For example, the ANOVA was initially developed within the context of experimental work (i.e., RS from one population, followed by RA to groups, followed by different treatments per group, followed by a test of the means to ascertain whether or not the means were *differentially* affected by the treatments), but is now routinely applied to quasi-experimental work (i.e., RS from different populations, followed by a test of the means to ascertain whether or not the *different* populations have different means). The assumptions of the ANOVA are less assured with quasi-experimental research. More specifically, the ANOVA was designed for the case of a ratio DV, but is routinely used with ordinal DVs (see Howell, p. 341). The ANOVA treats an ordinal DV *as if* it is interval, but that primarily has consequences for interpretation. An ordinal DV likely has more measurement error (i.e., it can be seen as an interval DV with low reliability), but that usually manifests as lower power (i.e., higher variance within each group) and less significance: When the DV is poorly defined, the power of the ANOVA is comparable to the power of the corresponding non-parametric tests and in extreme cases may actually be lower. The ANOVA was developed with the assumption of a normal population. However, this can be relaxed to unimodal populations (i.e., not bimodal) and if all groups have same population distribution (always the case for experimental research), the ANOVA is hardly affected. Bimodal (or multi-modal) distributions create particular problem for interpretation because the ANOVA is focused on differences between the means, and yet, in such cases, most people are *not* near the mean. The ANOVA is not particularly sensitive to the assumption of homogeneity of variances. For example, one guideline is that the largest variance can be up to 4 times the smallest variance. Some writers include “=n” (equal sample sizes per group) as an assumption but this is simply not true (but see power).

Assumptions should be checked and can be assessed “theoretically” or “empirically”. A

theoretical check involves consideration of the level of measurement and the research design to decide whether or not the assumption is reasonable. An empirical check involves looking at the data to assess the assumption. Theoretical checks must be applied to the level of measurement (i.e., the DV) and to the assumption of random sampling (a.k.a. independence): These are design issues. Theoretical checks may be applied to normality and homogeneity (i.e., consideration of whether or not the distributions would be bimodal or heterogeneous).. Empirical checks can be applied to normality and homogeneity, but one must be cautious because sample size has an impact. The Kolmogorov–Smirnov test is a standard test to assess normality (available in SPSS), but it has low power (less than 0.5) for samples less than about 750 (see Razali & Wah, 2011) and very low power (less than 0.1) for samples less than 100. The current data is limited to 44 cases. One can also check the distributions “by eye”. The Levene test is a standard test for homogeneity, and it is automatically provided by SPSS. However, it is considered more sensitive to homogeneity than the corresponding ANOVA (see Howell, 1997, p. 341). These were checked for each analysis, and issues are noted (if any) with each.

Dichotomous variables within ANOVA represent a special case. Dichotomous variables can be used in ANOVA if those variables represent an underlying continuum. In such cases, they represent a 2-point Likert scale (an ordinal scale). Dichotomous variables are modeled by a binomial distribution, but the binomial distribution may be approximated by a normal distribution (see Howell, 1997, p. 133) when  $p \approx 0.5$  (range approximately 0.2 to 0.8) and/or the sample size is high (typically greater than 30). This is the case herein. Exceptions are noted.

The test of the correlation is a parametric test. For the test of a correlation, the primary assumption is that the sample is a random sample (RS) from a single bivariate normal population with a correlation of 0 (often depicted as  $\rho = 0$ ). It is also assumed that both variables are measured on interval or ratio scales (though ordinal are commonly used). The test uses the sample correlation ( $r$ ) — the magnitude of the sample correlation — to reject (or “accept”) the assumption that the population correlation is zero. When plotted as a scatterplot, a bivariate normal distribution looks like an ellipse (football, cigar-shaped). The assumption of a bivariate normal distribution implicitly includes the assumption that the marginal distributions for X and Y are normal, that the conditional distributions for X on Y and Y on X are normal, and that the relationship between X and Y is linear. Again, there are other ways to express the assumptions. In particular, note that correlation is tightly related to regression, but the assumptions for

regression are expressed in slightly different ways (in practice, they reduce to the restrictions). Herein, the analyses are correlational, not regression. If the correlation is significantly different from zero, it is likely that all the assumptions are satisfied (it is difficult to achieve significance otherwise). However, if the correlation is not significantly different from zero, it is important to check the assumptions via the scatterplot — a non-significant correlation could arise because the relationship is non-linear. In the current work, all plots were checked using commands available in SPSS for creating a matrix of bivariate scatterplots. These are not included herein because of the amount of space required (there are hundreds of relationships to consider) and because they are not publication quality. Issues are noted at the time of analysis.

The assumptions of the chi-square include independent random sampling and the ability to classify each participant within a single category. These are both design issues. The chi-square also has concerns when the expected count per cell is less than 5. However, the solution is to use Fisher's Exact test which is routinely provided by SPSS. If the Fisher's test provides a different interpretation (the p-value will be different, but it only matters if the interpretation is different) than the "regular" chi-square, the Fisher test should be cited. In this work, both were noted but the Fisher test was not cited unless the results changed.

For all measures, it should be noted that all responses were bounded by questionnaire design. As such, issues of "outliers" (influential values) do not really apply.

Finally, all tests have concerns about power. Power is the ability to reject the null hypothesis if in fact that null hypothesis is false. Rejection of the null leads to acceptance of the alternative to the null. Given that the alternative to the null is usually the research hypothesis that the research is intended to support, power is important. However, in all statistics and particularly in the case of correlational designs (such as herein), the primary determinant of power is sample size. Since sample size is fixed once the data is collected, power cannot be changed. As such, it is important to retain as many participants as possible in subsequent analyses. Missing values become an important consideration. In addition, for the ANOVA (or t-test) power is also affected by the equality of group size. For a given sample size, the ANOVA has greater power if the samples have equal size. Unfortunately, in a design such as this, group sizes are determined by the data. At best, analyses can only exclude or combine small groups. Power is also affected by the heterogeneity of the sample (not under control in a correlational design) and by the distinctiveness of groups (again, not under control in a correlational design).

## 3.2 Results

### 3.2.1 Participant Demographics

A total of 75 participants (Public: 65; Student: 10) completed some of the survey. However, after data cleaning, the total sample size was reduced to 44 (see Section (3.2.2)). In the reduced sample, there were 25 females and 19 males (Public: 23 & 19; Student: 2 & 1). There was a no significant difference on gender between the two groups when using a chi-square test  $\chi^2(1) = 0.127$  ( $p < 0.721$ ).

Mean age (in levels) was 1.88 (SD: 0.92), with a mean of 1.88 (SD: 0.93) for the Public and a mean of 2.00 (SD: 1.00) for the Student group. Both means are in the 18 – 27 range. There was no significant difference on age between the two groups with  $t(42) = 0.219$  ( $p < 0.828$ ).

Mean educational level was 3.39 (SD: 1.35) with a mean of 3.34 (SD: 1.33) for the Public and a mean of 4.00 (SD: 1.74) for the Student group. Both means are in the “college or university undergraduate” range. There was no significant difference on education between the two groups with  $t(41) = 0.868$  ( $p < 0.139$ ).

Mean self-reported comfort with technology was 1.64 (SD: 0.85), with a mean of 1.69 (SD: 0.86) for the Public sample, and a mean of 1.00 (SD: 0.00) for the Student sample. Both means are in the “very comfortable” range. There was no significant difference between the two groups with  $t(40) = 1.374$  ( $p < 0.177$ ).

Mean self-reported knowledge of security was 1.295 (SD: 0.851) with a mean of 1.244 (SD: 0.860 for the Public sample (“minimal knowledge”), and a mean of 2.00 (SD: 0.00) for the Student sample (“good/secure”). There was no significant difference on knowledge between the two groups with  $t(42) = 1.507$  ( $p < 0.139$ ). Hereafter, the two samples were combined because of the small sample size for the Students ( $N = 3$ ) and the lack of significant difference.

The 44 respondents currently resided in Canada (11), Saudi Arabia (13), the UAE (1) or the USA (19), with 1 missing value. Family homes consisted of Canada (1), Egypt (3), Iraq (1), Nigeria (1), Saudi Arabia (25), South Africa (1) or the USA (10) with 2 missing values.

### 3.2.2 Data Cleaning

To simplify the process for participants, most of the items in the questionnaire used a “yes/no checklist” approach. The respondent checked a box if the item applied. Zero (0) was used as a default value. In this case, we cannot know if the participant skipped the item, or decided not to answer.

The items that did not use a checklist, the default was not zero. Therefore, the values of these items recorded as missing values and means that the participants did not respond. One such variable was the use of apps (e.g., Periscope use, YouNow use, Meerkat use and Other use), coded on a seven-point scale from “Never” (0) to “Several times a day” (6). If the respondent indicated the use of *at least one* app, then the missing values for all other apps were set to zero. On the other hand, if all the apps had missing values, then all were retained as missing values. Of the 75 respondents, 30 were missing on all. Of the remaining 45, one indicated no use of any app (i.e., the level of use for all apps was recorded as 0, or “never”). As such, there were only 44 useable responses for this item.

Another variable was the reported mood while broadcasting (Happy, Sad, Angry, Worried, Under Stimulants, when Compelled [e.g., work], and when Driving) coded on a five-point scale from 0 (“Never”) to 4 (“Always”). If the respondent indicated *at least one* mood while broadcasting, then the missing values for all other moods were replaced with zeros (0). If responses were missing for all 7 values (all moods), those values were considered as missing. 33 respondents were missing on all 7, but this included the 30 that were missing on app use. Of the respondents, the number of missing values were 1 (4 respondents), 2 (2 respondents), 3 (1 respondent), 5 (2 respondents) and 6 (3 respondents).

A third variable was the reported concerns (Social, Physical, Economic, Theft of Work, Use of Screenshots, Control over Viewing, Control over Location Viewing, Lawsuits, and Employer Monitoring) code on a 4-point scale from 0 (“Never thought about it”) to 3 (“Very Concerned”). If the respondent indicated *at least one* concern while broadcasting, then the missing values for all other concerns were replaced with ones (1). If responses were missing for all 9 values, those values were considered as missing. 34 respondents were missing on all 9, but this included the 33 that were missing on mood. Four respondents were missing on 1(Social) of the 9 values.

Collectively, these three items functioned as a check on responding. These items were distributed throughout the questionnaire (the app use was near the beginning, the concerns were near the end). If all these items were coded as missing values (i.e., the 4 app use, the 7 mood and the 9 concerns), then it was reasonable to assume that the respondent did not complete the questionnaire despite clicking the “submit” button. After applying these checks, the number of respondents was reduced to 45. Of that, one indicated that they never used any app, which was the main inclusion criterion. This left 44 participants who provided useful data (two were incomplete on the moods section, but useful). At the end of data cleaning there were 44 usable respondents of that 44, 37 provided complete data.

### 3.2.3 Apps Used

Use of Periscope YouNow, Meerkat and Periscope or “other apps” was coded on a 7-point scale as “Never” (0), “Less than once a month” (1), “Once a month” (2), “Once a week” (3), “Several times a week” (4), “Once a day” (5), and “Several times a day” (6). The number of users and the amount of use (Frequency) are provided in Table 3.1. Periscope was the most popular. It was also the most heavily used with a mean of 2.02, which corresponds usage that is between “Once a month” and “Once a week”.

Table 3.1 Use of Apps

App	Any Use	Exclusive Use		Frequency (Intensity of Use)			
		<i>N</i>	%	Mean	SD	Min	Max
Periscope	28	16	57.1	2.02	2.12	0	6
YouNow	13	6	46.2	0.68	1.27	0	5
Meerkat	14	7	50.0	1.30	2.18	0	6
Other	8	2	25.0	0.73	1.72	0	6

In Table 3.1, *Exclusive* is the number of respondents who used that app exclusively. For example, of the 28 users of Periscope, 16 (57.1%) used Periscope exclusively. Of the 44 respondents, 31 reported the use of a single app, 8 reported the use of two apps, 4 reported the

use of three apps and 1 reported the use of four apps. The mean number of apps used was 1.43 (SD: 1.00). Eight respondents cited the use of another app but only five identified those apps (“Blab”, “Snapchat” and “Facebook Live”). The individual who endorsed Snapchat (not a true Live Video Broadcasting app) also endorsed Periscope, Meerkat and YouNow. Although the small sample size for the student precludes prevent meaningful analysis, the two groups (Public vs. Student) did not differ on any measure using a two-group t-test or chi-square.

App use was collected as both type (Periscope, YouNow, Meerkat and Other) and intensity (on a 7-point scale) and 31 of 44 respondents used just one app. “To simplify later analyses, AppGrp was coded as a single variable with 5 levels: 1 (Periscope exclusive), 2 (YouNow exclusive), 3 (Meerkat exclusive), 4 (Other exclusive), and 5 (Multiple, non-exclusive, use). Subsequent analyses used this as an IV for analyses. AppIntensity was coded as the maximum level of use in any one category. This may underestimate the level of use in the Multiple group but only if those individuals should use multiple apps concurrently (within a single month). Table 3.2 presents the ANOVA for AppIntensity as a function of AppGrp.

Table 3.2 Means and Analysis of Group Differences for Maximum Intensity of Use.

	AppGrp					Analysis		
	Periscope	YouNow	Meerkat	Other	Multiple	<i>F</i>	<i>p</i> ( <i>F</i> )	$\eta^2$
N (Sample size)	16	6	7	2	13			
AppIntensity	3.75	2.83	5.14	4.50	3.31	2.013	0.112	0.171

Notes:  $df=(4,39)$

Note that there was no significant difference in mean intensity of use. All apps were used as the same intensity.

### 3.2.4 Reasons for Use

Respondents were asked, “Why did you start (or join) a live streaming video app? (Select all that apply)” with a subsequent yes/no checklist. Table 3.3 presents the individual reasons, and the percentage endorsement. In addition to the cited reasons, respondents could add their own. Four

stated reasons related to entertainment (“entertainment”, “for fun”, “to waste my free time”, “to know what is going on in the world”), one stated a reason that was consistent with a category that had been checked (“to maintain contact with my family and friends back home”), one was consistent with business promotion (“to find professional people and learn from them”) and recoded as such, and one was consistent with advising young people (“teach entrepreneurs how to start, build, run, and succeed in business”) and recoded as such, A final reason stated was “a family member of mine works for Periscope”). As such, two additional reasons were added to the list of reasons (in italics in Table 3.3).

Table 3.3 Reasons for Using Live Streaming Video Apps.

	Option	<i>N</i>	Endorsement (%)
1	to maintain contact with friends I know online	19	43.2
2	to maintain contact with friends I know offline	6	13.6
3	to maintain contact with strangers online	5	11.4
4	to find new friends online	18	40.9
5	to find new followers/fans online	12	27.3
6	to advocate for change	4	9.1
7	to help people in need (e.g. who suffer from depression)	7	15.9
8	to advise young people	5	13.6
9	to promote my professional profile	5	13.6
10	to promote my business or activities that I am involved in	6	13.6
11	to promote my events or event that I am involved in	2	4.5
12	<i>for entertainment</i>	4	9.1
13	<i>for other reasons</i>	1	2.3

On average, respondents indicated 2.07 (SD 1.23) reasons for the use of such apps; 42.3% indicate some type of business or commercial use, while 52.3% indicated some form of relationship seeking use.

Table 3.4 provides the Pearson correlations (*r*) between reasons for use (reasons are somewhat abbreviated from Table 3.3).



Table 3.4 Correlations between Reasons for Use.

		Reason Number											
		2	3	4	5	6	7	8	9	10	11	12	13
1	Friends Online	0.19	0.12	-0.17	-0.12	0.04	0.00	0.19	0.19	-0.08	0.03	-0.12	0.18
2	Friends Offline		0.07	<b>-0.33</b>	-0.10	-0.13	0.01	0.04	0.04	-0.16	-0.09	0.11	<b>0.38</b>
3	Strangers			<b>-0.30</b>	0.26	-0.11	-0.16	-0.14	0.28	-0.14	-0.08	-0.11	-0.06
4	New Friends				-0.09	0.06	0.02	-0.20	-0.20	-0.06	-0.18	-0.10	-0.13
5	New Followers					-0.02	-0.13	-0.10	-0.10	0.05	0.11	-0.19	-0.09
6	Advocate Chg						<b>0.30</b>	0.11	0.11	<b>0.34</b>	-0.07	-0.10	-0.05
7	Help							<b>0.37</b>	-0.17	0.01	-0.10	0.08	-0.07
8	Advise								0.04	0.04	0.23	-0.13	-0.06
9	Professional									0.23	<b>0.55</b>	-0.13	-0.06
10	Promote Bus										0.23	-0.13	-0.06
11	Promote Events											-0.07	-0.03
12	Entertainment												-0.05

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

Rounding makes the same value ( $r = 0.30$ ) seem significant sometimes and not others.

These are equivalent to Phi-coefficients ( $\Phi$ )

The average correlation was just  $r = -0.003$  (SD: 0.164, min: -0.331, max: 0.549), the mean *absolute* value of the correlations was only  $|r| = 0.131$  and the mean of the squared correlations was  $r^2 = 0.026$ . Most are small, but a few are moderate. This implies that the cited reasons were not tightly associated (i.e., they are independent). Only 6 of the 78 were significant. Note that if a chi-square test had been applied (based on the phi coefficient; see Section 3.1.5: Analytic Plan and General Comments on Issues for Statistical Analyses ), *all* of the significances would be the same.

Self-promotion for Events was correlated with Self Promotion for Professional reasons ( $r = 0.549$ ). Self-promotion for Business was correlated with Advocating for Change ( $r = 0.335$ ). Providing Help was correlated with Providing Advice ( $r = 0.370$ ). Finding New Friends Online

was *negatively* correlated with Maintaining Contact with Friends Offline ( $r = -0.331$ ) and *negatively* correlated with Maintaining Contact with Strangers Online ( $r = -0.298$ ). The last significant correlation involved the other category. To summarize the correlation matrix, there does seem to be a trend for some individuals to have used these apps to promote their work or profession (Self Promote for Professional Reasons, for Business or for Event plus Offer Advice). Other individuals used these apps to find new friends, or to maintain contact with existing friends (Friends Offline, Friends Online, Strangers). Still others used these apps to advise and provide help (Offer Advice, Offer Help). A final group of individuals used these apps to find new friends or followers (Find New Friends or Find New Followers), although these could be two separate groups (i.e., the only positive correlation for Find New Friends is with Find New Followers, but it is small and non-significant). It is interesting that those who used such apps to maintain contact with old friends did *not* use these apps to find new friends (and vice versa): The correlations are negative. In future work, one could combine variables to create four main groups: Maintaining Friends and Associations, Maintaining Business or Professional Associations, Helping and Advocating for Change, and Making New Friends/Followers. These groups are not completely independent (they overlap somewhat) but seem sufficiently delineated to be useful.

### **3.2.5 Categories of Use**

Participants were asked about the nature of their broadcasts using a yes/no checklist format. Data was collected within five categories: Formal Broadcasts of Self, Informal Broadcasts of Self, Formal Broadcasts of Others, Informal Broadcasts of Others and Non-Human Broadcasts (broadcast that did not focus on humans), For each category data was collected within three levels of audience (Private to a Single Person, Private to Multiple Persons, and Public), within two levels of planning (Planned and Spontaneous), within five levels of location (Work, Home, Public, Parties, and while Driving) and within seven levels of mood (Happy, Sad, Angry, Worried, Compelled, and Stims). The last two are included as moods because being compelled to create a broadcast should render mood irrelevant, while stimulants (e.g., alcohol and recreational drugs) are mood-altering.

Table 3.5 presents the type of audience. The number under Any is the number who endorsed private or public (or both). The number under “Private” and “Public” the total number

of respondents who endorsed the option, while the percentage is the proportion of individuals within each broadcast type (i.e., 44.8% of the 29 users [13 of 29] who created Formal Broadcasts of Self did so for a public audience).

Table 3.5 Categories of Broadcasts (BCs) and the Types of Audience for Each Category.

Category of BC	Any		Private				Public	
			Single		Multiple			
	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%
Formal BCs of Self	29	64.4	2.0	6.9	8.0	27.6	13.0	44.8
Informal BCs of Self	35	77.8	5.0	14.3	11.0	31.4	15.0	42.9
Formal BCs of Others	26	57.8	4.0	15.4	7.0	26.9	3.0	11.5
Informal BCs of Others	29	64.4	4.0	13.8	11.0	37.9	4.0	13.8
Non-Human BCs	22	48.9	1.0	4.5	4.0	18.2	12.0	54.5
Any Category	44	95.6	8	18.6	23	53.5	26	60.5

Notes: Total sample size is 43.

There were more Broadcasts of Self (Formal or Informal). Within categories, Public broadcasts dominate for the Formal or Informal Broadcast of Self, while Private dominates for the Formal or Informal Broadcasts of Others. Across categories, most are Public.

Most participants (76.7% of 43 who completed this section) engaged in a mix of broadcast types and 41.9% engaged in all five types. The mean number of categories selected was 3.28 (SD 1.68). Broadcasts of Self (Formal or Informal) were endorsed by about 93.0% of respondents (of 43), while Broadcasts of Others (Formal or Informal) were endorsed by 74.4%. Informal Broadcasts (Self or Other) endorsed by 86.1% of respondents while Formal (Self or Other) were endorsed by 74.4%.

Of the 43 respondents, 2.3% exclusively engaged in Broadcasts of Non-Human topics, 20.9% exclusively engaged in Broadcasts of Self (Formal or Informal), 4.7% exclusively engaged in Broadcasts of Others (Formal or Informal) and 72.1% engaged in a mix of Broadcasts of Self and Others. Note that Broadcasts of Non-Human topics have few issues of privacy and security (though human may be caught in the background, the broadcaster may reveal his/her

location or other details). Broadcasts of Self have fewer issues of privacy and security (because there is more control and because others are not involved). However, the remaining 77% of broadcasts need to be concerned about privacy and security.

From another perspective, the same 2.3% exclusively engaged in Non-Human Broadcasts, 11.6% exclusively engaged in Formal Broadcasts, 20.9% exclusively engaged in Informal Broadcasts and 65.1% engaged in both Formal and Informal Broadcasts.

Table 3.6 presents the correlations between any broadcast use within Categories.

Table 3.6 Correlations between Categories of Broadcasts (BCs)

	Formal BCs of Self	Informal BCs of Self	Formal BCs of Others	Informal BCs of Others	Non-Human BCs
Formal BCs of Self	1.000	0.111	<b><i>0.572</i></b>	0.090	<b><i>0.527</i></b>
Informal BCs of Self		1.000	<b><i>0.380</i></b>	<b><i>0.467</i></b>	<b><i>0.394</i></b>
Formal BCs of Others			1.000	<b><i>0.572</i></b>	<b><i>0.555</i></b>
Informal BCs of Others				1.000	<b><i>0.432</i></b>
Non-Human BCs					1.000

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 43$  for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The average correlation was  $r = 0.410$  (SD: 0.178, min: 0.090, max: 0.572), the average of the absolute values was  $|r| = 0.410$ , and the average squared correlation was  $r^2 = 0.196$ . These are moderate in size, implying fairly strong relationships. Most (8 of 10) are significant ( $p < 0.05$ ). The highest  $r = 0.572$  implies that those who engage in Formal Broadcasts of Self also engage in Formal Broadcasts of Others. Similarly, the  $r = 0.467$  implies that those who engage in Informal Broadcasts of Self also engage in Informal Broadcasts of Others. The only non-significant correlations imply that those who engage in Formal Broadcasts of Self do *not* have a tendency to engage in Informal Broadcasts of Self, or Informal Broadcasts of Others (that is, they do “formal broadcasts” only). Those who engage in Non-Human Broadcasts, also engage in other types.

From the previous Table 3.5, we can see that most broadcasts are public, and very few are private to a single person. Because the numbers under Private-Single were low, the two

levels of Private were combined. Any respondent who endorsed Private-Single and/or Private-Multiple was considered Private. The data of Table 3.5 are adjusted and presented in Table 3.7.

Table 3.7 Categories of Broadcasts (BCs) and the Adjusted Types of Audience for Each Category

Category of BCs	Any		Private		Public		Exclusive				Both	
							Private		Public			
	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%
Formal BCs of Self	29	64.4	10	34.5	13	44.8	9	31.0	12	41.4	1	3.4
Informal BCs of Self	35	77.8	15	42.9	15	42.9	15	42.9	15	42.9	0	0.0
Formal BCs of Others	26	57.8	11	42.3	3	11.5	11	42.3	3	11.5	0	0.0
Informal BCs of Others	29	64.4	15	51.7	4	13.8	15	51.7	4	13.8	0	0.0
Non-Human BCs	22	48.9	5	22.7	12	54.5	5	22.7	0	0.0	0	0.0
All Categories	43	95.6	24	55.8	26	60.5	14	32.6	13	30.2	10	23.3

Notes: The sum of Exclusive, Private, Exclusive: Public, and Both may not equal the total because of missing values.

Table 3.7 also includes the number within each category who was exclusively Private, exclusive Public, or both Private and Public. It is the Public broadcasts that have more concerns for privacy and security.

Broadcasts of Self seem to be evenly split between Private and Public, whereas Broadcasts of Others tend to be Private. Within the categories, respondents tended to use either Private or Public broadcasts. However, when considering all categories of broadcasts, respondents were more variable. Across all categories, 33% only engaged in Private broadcasts, 30% only engaged in Public broadcasts, and 23% engaged in both Private and Public broadcasts. It is the 53% that engaged in some level of Public broadcasts that are a primary issue for security and privacy. A further 15.9% did not provide any information about the type of audience although they had indicated the category of broadcasts. These respondents were included in the totals per category, but not in the Private or Public values. As such, the values for Private and Public might be slight underestimations.

Table 3.8 provides the degree of planning associated with each type of broadcast. The

*Any* is repeated from Table 3.5 to provide context. Within each category, respondents could indicate that broadcasts were planned *and/or* spontaneous (i.e., they could choose both) but no respondent indicated both within a single category. Again, all values are expressed as the proportion of individuals within each broadcast type (i.e., 58.6% of the 24 users who created Formal broadcast of Self planned those broadcasts). Neither are the respondents who did not indicate either planned or spontaneous broadcasts.

Table 3.8 Categories of Broadcasts (BCs) and the Types of Planning for Each Category.

Category of BCs	Any		Planned		Spontaneous		Neither	
	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%
Formal BCs of Self	29	66.0	17	58.6	9	31.0	3	10.3
Informal BCs of Self	35	80.0	6	17.1	26	74.3	3	8.6
Formal BCs of Others	26	59.0	12	46.2	11	42.3	3	11.5
Informal BCs of Others	29	66.0	7	24.1	18	62.1	4	13.8
Non-Human BCs	22	22.0	3	13.6	16	72.7	3	13.6
Any Category	44		25	58.1	32	74.4	4	9.3

Notes: Total sample size for categories was 43, but the total samples size for planning was 44.

Four respondents did not indicate any type of planning (both planned and spontaneous were zero across all Categories). Planning is more common with the Formal broadcasts (endorsed by about 52% of respondents) than with the Informal broadcasts (about 21%). Conversely, Spontaneity is more common with Informal Broadcasts (about 68%) than with Formal Broadcasts (about 37%). Overall, spontaneity, which is a greater concern in terms of privacy and security, was more commonly reported than planning. Furthermore, across all categories, only 4.5% (2) indicated that *all* broadcasts were planned, whereas 13.6% (6) indicated that *all* broadcasts were spontaneous and 72.7% (32) indicated a mix of planned and spontaneous broadcasts (9.1% or 4 respondents did not provide data).

Table 3.9 provides the data related to the location of the broadcasts. All values are expressed as the proportion of individuals within each broadcast type (i.e., 44.8% of the 24 users who created Formal Broadcast of Self did so at work).

Table 3.9 Categories of Broadcasts (BCs) and the Locations of those Broadcasts.

Category of BCs	Any		Work		Home		Public		Parties		Driving	
	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%
Formal BCs of Self	29	67.4	13	44.8	18.0	62.1	11.0	37.9	7.0	24.1	4.0	13.8
Informal BCs of Self	35	81.4	6	17.1	21.0	60.0	18.0	51.4	12.0	34.3	8.0	22.9
Formal BCs of Others	26	60.5	8	30.8	8.0	30.8	16.0	61.5	3.0	11.5	4.0	15.4
Informal BCs of Others	29	67.4	6	20.7	9.0	31.0	14.0	48.3	12.0	41.4	4.0	13.8
Non-Human BCs	22	22.0	5	22.7	9.0	40.9	9.0	40.9	5.0	22.7	4.0	18.2
Any Category	44		17	39.5	34	79.1	29	69.8	17	39.5	11	26.5

Notes: Total sample size for categories was 43, but the total samples size for locations was 44.

Firstly, most broadcasts are conducted at home (endorsed by about 79% of participants) or in public places (endorsed by about 70%). broadcasts at work (about 40%) or at parties (about 40%) are lower. Broadcasts while driving are relatively low (endorsed by about only 17% of respondents). Most of the categories followed the same pattern, although there were some notable exceptions. Informal Broadcasts of Others were more commonly reported to occur at parties than at home or work.

There were five different locations. Collapsed over Categories of Broadcast, respondents indicated the use of an average of 2.45 (SD: 1.41) different locations (range 0 to 5). However, within each category, the numbers were smaller with a means of 1.20 (SD: 1.42) for Formal Broadcasts of Self, 1.48 (SD: 1.39) for Informal Broadcasts of Self, 0.89 (SD: 1.06) for Formal Broadcasts of Others, 1.02 (SD: 1.05) for Informal Broadcasts of Others, and 0.73 (SD: 1.32) for Non-Human broadcasts. This is important because it implies that most respondents only used a type of location within each category, but multiple types of locations across categories. Table 3.10 presents the correlations between locations collapsed over Categories.

Table 3.10 Correlations between the Locations of Broadcasts.

	Work	Home	Public	Parties	Driving
Work	1.000	0.208	<b>0.374</b>	0.233	0.189
Home		1.000	-0.047	-0.015	-0.063
Public			1.000	<b>0.472</b>	-0.194
Parties				1.000	<b>0.404</b>
Driving					1.000

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The average correlation was  $r = 0.195$  (SD: 0.190, min  $-0.063$ , max: 0.472), the average of the absolute values was  $|r| = 0.220$ , and the average squared correlation was  $r^2 = 0.070$ . These are small in size, though the three significant correlations are moderate. As such, it seems that across categories, respondents do not use the same locations consistently. That is, the respondents who use the home for Informal Broadcasts of Self are not *necessarily* the same respondents who use the home for Formal Broadcasts of Self. Simply, there is little consistency. Those who broadcast in Public also broadcast from Work. Those who broadcast in Public tend to also broadcast at Parties. Those who broadcast while Driving tend to also broadcast at Parties (a strong implication for the entertainment aspect of broadcasting).

Table 3.11 shows the data related to mood while broadcasting. All values are expressed as the proportion of individuals within each broadcast type (i.e., 58.6% of the 29 users who created Formal Broadcasts of Self did so when happy).



Table 3.11 Categories of Broadcasts (BCs) and Mood while Broadcasting.

Category of BC	Any		Happy		Sad		Angry		Worried		Compelled		Stims	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Formal BCs of Self	29	67.4	17	58.6	1	3.4	1	3.4	9	31.0	7	24.1	1	3.4
Informal BCs of Self	35	81.4	31	88.6	6	2.9	6	2.9	6	25.7	8	20.0	0	0.0
Formal BCs of Others	26	60.5	15	57.7	0	23.1	2	23.1	5	23.1	5	30.8	2	7.7
Informal BCs of Others	29	67.4	22	75.9	1	0.0	4	6.9	3	17.2	7	17.2	1	3.4
Non-Human BCs	22	22.0	12	54.5	3	4.5	3	18.2	6	13.6	7	31.8	2	9.1
Any Category	43		38	88.4	8	18.6	8	18.6	14	32.6	21	48.8	3	7.0

Notes: Total sample size for categories was 43, but the total samples size for mood was 44.

Broadcasting while happy was endorsed by about 88% of respondents. Very few endorsed broadcasting while under the influence of stimulants (about 7%). However, there was substantial endorsement of broadcasting while angry (about 18%), particularly for broadcasts of Others, and while worried (about 33%). These two moods may be cause for concerns about security and/or privacy. A number of broadcasts (49%) were created when required to do so (this classification was intended to accommodate those who create broadcasts as a part of employment or other obligations, for which mood might be irrelevant).

Overall, respondents indicated an average of 4.39 (SD: 3.62) different moods. However, within categories the numbers were smaller with a means of 0.82 (SD: 0.72) for Formal Broadcasts of Self, 1.30 (SD: 1.39) for Informal Broadcasts of Self, 0.66 (SD: 0.83) for Formal Broadcasts of Others, 0.75 (SD: 1.30) for Informal Broadcasts of Others, and 0.75 (SD: 1.30) for Non-Human broadcasts.

Participants were also asked to provide a more general assessment of mood with an item

that asked, “How often do you broadcast when?” (happy/excited, sad/depressed, angry/frustrated, worried/anxious, intoxicated, compelled to share, or while driving). Responses were collected on a 5-point scale from “never” (0), through “rarely” (1), “sometimes” (2), “often” (3), to “always” (4). There was also a category for “not applicable” (coded as -2), which was treated as equivalent to “never” (coded as 0) in analyses. Missing values were possible: There were two participants who were missing on all 7 items. Table 3.12 presents the summary

Table 3.12 General Mood while Broadcasting.

	Mean	SD	Min	Max
Happy	3.07	1.09	0	4
Sad	0.60	0.86	0	3
Angry	0.76	0.98	0	4
Worried	0.88	1.04	0	3
Compelled	1.86	1.59	0	4
While Using Stimulants	0.21	0.52	0	2
While Driving	0.76	1.30	0	4

Notes: Total sample size is 42.

The data of Table 3.12 parallels the data of Table 3.11 in that most broadcasts are made when Happy. The next most commonly reported mood is Compelled (e.g., work required). Note that the maximum values for Angry, and While Driving are both 4 (“always”) indicating that respondents are always angry or driving while broadcasting.

Table 3.13 presents the correlations between overall mood (collapsed over categories of broadcast)

Table 3.13 Correlations between Moods while Broadcasting.

	Happy	Sad	Angry	Worried	Stimulants	Compelled	Driving
Happy	1.000	0.162	0.153	0.008	-0.114	0.048	0.270
Sad		1.000	<b><i>0.404</i></b>	<b><i>0.464</i></b>	0.199	0.279	0.130
Angry			1.000	0.162	<b>0.341</b>	0.197	0.126
Worried				1.000	0.184	0.093	-0.075
Stimulants					1.000	0.097	0.149
Compelled						1.000	<b>0.384</b>
Driving							1.000

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 42$  for all comparisons.

These are *not* equivalent to phi-correlations ( $\Phi$ ).

The average correlation was  $r = 0.174$  (SD: 0.148, min: -.114, max: 0.464), the average of the absolute values was  $|r| = 0.194$ , and the average squared correlation was  $r^2 = 0.051$ . These are small, though the four significant correlations are moderate. Note that Angry, Sad and Worried tended to be correlated, that Stimulants and Angry were correlated, and that Compelled and Driving were correlated. That is, those who broadcast when Angry tend to broadcast when under the influence of stimulants (though that use is rare) or when Sad. Those who broadcast when Sad tend to broadcast when Worried, and some people seem to be compelled to broadcast while driving — whether this is an external requirement (e.g., for work) or an internal compulsion is not clear.

A one-way within-subjects ANOVA showed that the mean frequencies for each mood differed with  $F(6,246) = 39.586$ ,  $p < 0.0005$ ,  $\eta^2 = 0.451$ . Follow-up tests showed the frequency for Happy > Compelled > Sad  $\approx$  Angry  $\approx$  Worried  $\approx$  Driving > Stimulants. Using the pooled error from the within-subjects ANOVA, the critical value for a significant difference between means would be 0.444 (i.e.,  $t_{crit}(1,40)=2.02$ ). However, it should be noted that the actual analysis used specific error terms, and as such had a slightly different critical values for each pair of moods..

Finally, in this section about use, an item addressed any restrictions on use using a yes/no checklist, while another two items probed knowledge about the ephemeral nature of the resulting

video (broadcast). Table 3.14 provides the results for the restrictions on use. Note that this analysis is based on 42 respondents (a total of 2 missing values for each).

Table 3.14 Restrictions on Use.

	N	%
Not Restricted	26	61.9
Nothing more to broadcast	5	11.9
Restricted by Available Time	8	19.0
Restricted by Data Plan	7	16.7
Restricted by Other Costs	1	2.4
Restricted by Issues of Security	5	11.9

Notes: Total sample size is 42.

One additional respondent added, “The only restriction I have is partial blindness.” Note that most respondents (61%) are using these apps to their capacity.

As to knowledge of the ephemeral nature of the video (broadcast), participants were asked, “Do you know that these apps do not enable the viewers to save the broadcasts?” Responses were collected as “yes”, “no” and “I know that Periscope allows one to save videos for up to 24hr (but the others do not).” Of the 40 respondents, 22.5% ( $N = 9$ ) said “no”, 42.5% ( $N = 17$ ) said “yes”, and 35.0% ( $N = 14$ ) claimed knowledge of Periscope. Respondents were also asked, “Do you know that these apps do not enable the viewers to replay the broadcasts?” with similar options of “yes”, “no” and “I know that Periscope allows one to replay videos for up to 24hr (but the others do not).” Of the 40 respondents, 27.5% ( $N = 11$ ) said “no”, 42.5% ( $N = 17$ ) said “yes”, and 30.0% ( $N = 12$ ) claimed knowledge of Periscope. “This was important information for the interpretation of subsequent items about concerns (security and privacy).”

### 3.2.6 Concerns and Issues

Participants were asked to rate their degree of “concern” in nine areas using a four-point scale (0 = “Never thought about it”, 1 = “Not at all Concerned”, 2 = “Concerned” and 3 = “Very

Concerned”). There were three respondents who did not complete this section. “Note that “never thought about it” was coded as 0 because it implies even less concern than “not at all concerned”.” For this analysis, the sample size was 41. Table 3.15 presents the results.

Table 3.15 Concerns (out of 3).

		Mean	SD	Min	Max
1	Social reputation	2.00	0.97	0	3
2	Physical harm (e.g., stalkers)	2.02	0.94	0	3
3	Economic harm (e.g., identity theft)	1.76	1.16	0	3
4	Others using or sharing my broadcasts without my consent	1.54	0.98	0	3
5	Others taking a screenshot of my face or appearance	1.78	1.08	0	3
6	Not knowing (or controlling) who views my broadcasts	1.73	0.81	0	3
7	Not knowing (or controlling) who views my location	2.15	0.85	0	3
8	Potential lawsuits from others in my broadcasts	1.22	0.96	0	3
9	Potential employers can and will monitor my broadcasts.	1.32	0.85	0	3

Notes: Means are based on 41 participants.

The mean rating across all concerns was 1.72 (SD: 0.50) indicating mild concern, with a minimum average rating of 0.78 and a maximum rating of 3.00 (i.e., some rated all concerns as a 3). Three areas prompted the highest level of concern with ratings above 2.00 (between “concerned” and “very concerned”): reputation, physical harm, and not knowing or being able to control who can view broadcaster location. The correlation matrix did revealed moderate associations (see Table 3.16), though none were large (i.e., all were  $r < 0.707$ ). “Note that the format of the table is altered from previous correlation matrices to provide more space. The redundancies are removed.

Table 3.16 Correlations between Concerns.

		Concern Number							
		2	3	4	5	6	7	8	9
1	Social	-0.137	<b>0.332</b>	-0.079	<b>0.331</b>	-0.032	0.180	0.160	0.091
2	Physical		0.144	<b>0.533</b>	0.104	-0.057	-0.036	-0.062	<b>0.336</b>
3	Economic			0.251	<b>0.474</b>	0.223	0.290	0.229	0.208
4	Unauthorized Use				0.138	0.187	0.023	-0.182	-0.029
5	ScreenShot Theft					0.302	0.063	0.095	<b>0.322</b>
6	Knowing Viewers						<b>0.530</b>	<b>0.335</b>	0.091
7	Controlling Location Viewers							0.204	0.176
8	Lawsuits								<b>0.555</b>

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

These are *not* equivalent to phi-correlations ( $\Phi$ ).

The average correlation was  $r = 0.175$  (SD: 0.189) with a maximum of  $r = 0.555$ , and a minimum of  $r = -0.182$ . The average of the absolute values was  $|r| = 0.209$ , and the average squared correlation was  $r^2 = 0.065$ . These are small, though the largest (significant) are moderate. Based on the pattern of the correlation matrix, the concerns can be grouped: Economic (Economic, ScreenShots, Controlling Viewers, Controlling Location Viewers, Employers), Serious Harm (Unauthorized Use, Physical Harm), and Social (Social). The Social tends to have weak associations with the other two groups.

A one-way within-subjects ANOVA was used to explore differences between concerns. Level of concern for each concern differed significantly with  $F(8,320) = 5.413$  ( $p < 0.0005$ ), though the effect size was not large ( $\eta^2 = 0.119$ ). Follow-up tests found that Controlling Location Viewers  $\approx$  Physical  $\approx$  Social  $>$  Screenshot Theft  $\approx$  Economic  $\approx$  Knowing Viewers  $\approx$  Unauthorized Use  $>$  Employers  $\approx$  Lawsuits. Using the pooled error from the within-subjects ANOVA, the critical value for a significant difference between means would be 0.390 (i.e.,  $t_{crit}(1,40) = 2.02$ ). However, it should be noted that the actual analysis used specific error terms, and as such had a slightly different critical values for each pair of concerns.

From a theoretical perspective, an alternative grouping might be “Personal Harm” (social harm, physical harm, economic), “Control over Audience” (controlling viewers, controlling location viewers, employers), and “Work or Intellectual Property loss” (screenshot theft, lawsuits). Note that these are reasonably aligned with the correlation matrix. Personal Harm had a mean rating of 0.772 (SD: 0.66). Control over Audience had a mean of 1.73 (SD: 0.60). Work or Intellectual Property Loss had a mean 1.51 (SD: 0.60). These more general assessments differed significantly with  $F(2,80) = 8.569$  ( $p < 0.0005$ ,  $\eta^2 = 0.176$ ).

With respect to concerns, participants were asked “When using temporal live video streaming apps, broadcasts are not permanently available on these apps for viewers. This is a positive feature because:” Responses were collected using a yes/no checklist of items and an open-ended response. The possible options and the degree of endorsement are provided in Table 3.17. The open-ended responses included “I can delete it when ever i [Sic] want and others wont [sic] see it” (recoded as privacy and secret, though it could imply other options), “I don't agree with any of the above information” (consistent with the lack of endorsement of every option) and “I just think it's a neat feature. You have to use the app regularly to keep up.” There (see Table 3.17) were 42 participants who completed this section.

Table 3.17 Endorsement of Positive Features of Ephemeral Nature of Broadcast

		<i>N</i>	%
1	keeps contents secretive	11	26.2
2	protects my privacy	24	57.1
3	protects my property	5	11.9
4	reduces unwanted viewers	14	33.3
5	enables people to forget me	5	11.9
6	prevents profiling me	12	28.6
7	minimized data companies collect about me	7	16.7
8	protects privacy of others	10	23.8
9	minimizes data companies collect about others	7	16.7

Notes: Total sample size is 42.

By far the most common reason, with 57.1%, was that it protects the broadcaster's privacy; the next most common reason was that it reduces the presence of unwanted viewers. The mean number of cited positive features was 2.21 (SD: 1.73; range 0 to 7). Hence, most respondents picked at least two. Table 3.18 presents the correlations between Positive Features.

Table 3.18 Correlations between Positive Features of the Ephemeral Nature of Broadcasts.

	2	3	4	5	6	7	8	9
1 keeps contents secretive	0.105	-0.041	0.169	0.289	0.118	<b>0.323</b>	<b>0.313</b>	0.179
2 protects my privacy		-0.248	0.036	<b>0.327</b>	-0.158	-0.102	-0.267	<b>-0.476</b>
3 protects my property			0.063	-0.128	<b>0.424</b>	0.236	<b>0.318</b>	0.236
4 reduces unwanted viewers				-0.245	0.239	0.236	0.212	0.103
5 enables people to forget me					-0.058	-0.156	-0.194	-0.156
6 prevents profiling me						<b>0.431</b>	<b>0.520</b>	<b>0.431</b>
7 minimized data companies collect about me							<b>0.505</b>	<b>0.490</b>
8 protects privacy of others								<b>0.505</b>

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ )

The average correlation was  $r = 0.127$  (SD: 0.263, min  $-0.476$ ; max 0.520). The mean absolute value was  $|r| = 0.251$ , which was small. There were 11 significant correlations. Overall, the pattern of correlations implies two distinct groups. One group endorses Protects my Privacy and Enables People to Forget Me, while the other group endorses the rest.

In a similar style, participants were asked “When using temporal live video streaming apps, broadcasts are not permanently available on these apps for viewers. This is a negative feature because:” Responses were collected using a yes/no checklist of items and an open-ended item. The possible options and the degree of endorsement are provided in Table 3.19. The open ended responses included “The problem with broadcasts not being able to be saved for later is suppose one of my friends can't listen while I'm live. Once the stream ends, that's it. They can't hear what happened. I have to use a different service to record my meerkat streams so people ...”



(consistent with endorsement of number of viewers), “Special people ' family members' would like to have the video for their records.” (Consistent with the endorsement of valuable) and ”Other tools are available to download videos, Katch/Fullscope and other 3rd party screen capture. Privacy does not exist.” Table 3.19 presents the results.

Table 3.19 Endorsement of Negative Features for Ephemeral Nature of Broadcast

		<i>N</i>	%
1	content could be valuable	22	52.4
2	cannot know who watched broadcast	17	40.5
3	reduces number of viewers	12	28.6
4	need to recreate for each broadcast	9	21.4
5	enable people to forget me	5	11.9
6	limits potential popularity of broadcast	8	19.0

Notes: Total sample size is 42.

The major concern is that it could be valuable. The mean number of cited negative features was 1.69 (SD: 1.04; range 0 to 4). Although the mean implied the respondents select only one or two features, the correlation matrix is provided in Table 3.20.

Table 3.20 Correlations between Negative Features of the Ephemeral Nature of Broadcasts.

		2	3	4	5	6
1	content could be valuable	<b>-0.327</b>	0.102	-0.169	-0.215	<b>-0.354</b>
2	cannot know who watched broadcast		0.143	0.292	0.010	0.231
3	reduces number of viewers			0.069	0.102	-0.024
4	need to recreate for each broadcast				-0.182	<b>0.345</b>
5	enable people to forget me					0.017

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The average correlation was  $r = 0.003$  (SD: 0.215, min  $-0.354$ ; max 0.345). The mean absolute value was  $r = 0.172$ , which was small. The correlations imply that those who are concerned about the value of the content are *not* concerned about knowing who watched, or about limits on the popularity of the broadcast. Those who are concerned about popularity are also concerned about the need to recreate.

The number of positive features endorses was *positively correlated* ( $r = 0.369, p < 0.004$ ) with the number of negative features.

On the topic of concerns, participants were asked “With respect to feedback about viewers, I would like the app to (choose all that apply):” Responses were collected using a yes/no checklist and an open-ended item. The options (simplified) are presented in Table 3.21.

Table 3.21 Endorsement of Feedback Options

	<i>N</i>	%
1 notify me about who viewed my GPS location	34	81.0
2 identify viewers	20	47.6
3 identify followers	20	47.6
4 block viewers who take screenshots of my broadcast	24	57.1

Notes: Total sample size is 42.

Almost everyone wants to be notified about who checks the GPS location, and most want the ability to block viewers who take screenshots of broadcasts. One individual specifically stated “Notifying me who exactly is close to where i [sic] am” (consistent with the endorsement of the GPS location option). The correlations are presented in Table 3.22.

Table 3.22 Correlations between Feedback Items

	2	3	4
1 notify me about who viewed my GPS location	0.059	0.059	0.050
2 identify viewers		<b>0.725</b>	<b>0.467</b>
3 identify followers			0.283

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

There are particularly strong correlations between the desire to identify viewers, to identify followers, and to block viewers who take screenshots. The pattern of correlations show that there are 2 groups; those who want GPS and those who want information about viewers.

More specific ideas were explored with an item that asked, “In broadcasts, would you like to keep the following sensitive information private (choose all that apply)?” Responses were collected using a yes/no checklist and an open-ended item. The options. (Simplified) are presented in Table 3.23. One respondent stated, “I really wish periscope just said my city or county” (consistent with their endorsement of exact GPS).

Table 3.23 Endorsement of Options about Information that is Sensitive (to be Kept Private)

		<i>N</i>	%
1	my face	13	31.0
2	my voice	6	14.3
3	my exact GPS location	28	66.7
4	my approximate location	10	23.8
5	the visual of my surroundings	5	11.9
6	the people in my surroundings	11	26.2
7	my inappropriate behavior	19	45.2
8	the inappropriate behavior of others	6	14.3

Note that the only option with high endorsement in location. The second highest is inappropriate behavior, though that might be difficult to achieve with current technology (and requires a definition of “inappropriate”). The mean number of items or Sensitive Information was 2.22 (SD: 1.54, min: 0; max 8). Table 3.24 provides the correlations.

Table 3.24 Correlations between Information that is Sensitive (to be Kept Private)

		2	3	4	5	6	7	8
1	hide face	0.178	<b>0.386</b>	0.005	0.082	0.201	0.039	0.033
2	hide voice		0.025	0.259	0.275	0.229	-0.213	0.035
3	hide GPS			0.184	-0.027	0.218	-0.104	-0.250
4	hide location				<b>0.318</b>	0.188	-0.144	0.101
5	hide visuals					0.289	-0.023	0.275
6	hide people						0.026	0.076
7	hide bad behavior: me							<b>0.322</b>

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The average correlation was  $r = 0.107$  (SD: 0.166, min  $-0.250$ ; max 0.386). The mean absolute value was  $r = 0.161$ , which was small. There are only 3 significant correlations, and they are not strong (hiding face with hiding GPS; hiding general location with hiding surrounding visuals; hiding my inappropriate behavior with hiding inappropriate behavior of others).

Reasons for hiding one’s face or voice were collected using a yes/no checklist and one open-ended item. The content of open-ended item was recoded into one of the existing codes if possible. The cited reasons for hiding (or distorting) one’s face or voice are presented in Table 3.25. For face hiding, the comments included “Religion Reasons.” and “Sometimes I dont [sic] feel like making myself up to be seen on live stream....” (This individual did not endorse “personal reasons” so it was not recoded). For voice hiding, one individual commented “My accent is easily identified.” but it was unclear if this implied a personal social or professional reason, so it was not recoded. Note that none are particularly high, and that ID Theft is the highest concern.

Table 3.25 Endorsement of Options citing Reasons to Hide Face or Voice

	Face		Voice	
	<i>N</i>	%	<i>N</i>	%
ID Theft	19	45.2	11	26.2
Stalkers	14	33.3	7	16.7
Professional reasons (e.g., BCs are incompatible with employment)	10	23.8	6	14.3
Social reasons (e.g., BCs are incompatible with social class)	10	23.8	6	14.3
Personal reasons (e.g., not attractive)	4	9.5	6	14.3

Table 3.26 provides the correlations between reasons for hiding face, and the reasons for hiding voice.

Table 3.26 Correlations between Reasons to Hide Face and Voice.

		Face				Voice				
		stalkers	professional reasons	social reason	personal reasons	ID theft	stalkers	professional reasons	social reason	personal reasons
Face	ID theft	<b>0.488</b>	<b>0.513</b>	-0.035	0.044	<b>0.556</b>	0.248	<b>0.322</b>	-0.213	0.055
	stalkers		<b>0.445</b>	0.212	-0.046	0.282	<b>0.503</b>	0.155	0.155	0.155
	professional reasons			-0.035	0.206	<b>0.313</b>	<b>0.357</b>	<b>0.733</b>	0.101	0.417
	social reason				0.206	0.188	0.209	0.101	<b>0.575</b>	0.259
	personal reasons					0.000	0.295	<b>0.335</b>	0.105	<b>0.796</b>
Voice	ID theft						<b>0.466</b>	<b>0.535</b>	0.076	0.076
	stalkers							<b>0.551</b>	0.189	<b>0.370</b>
	professional reasons								0.228	<b>0.421</b>
	social reason									0.228

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

For the correlations between reasons to hide face, the average correlation was  $r = 0.200$  (SD: 0.220, min -0.046; max 0.513). The mean absolute value was  $|r| = 0.176$ , which was small. For the correlations between reasons to hide voice, the average was  $r = 0.132$  (SD: 0.134, min -0.084; max 0.303). The mean absolute value was  $|r| = 0.163$ , which was small.

What more interesting is the correlations between the complementary reasons to hide face or voice. They are all high. For example, hiding face for personal reasons is strongly correlated ( $r = 0.796$ ) with hiding voice for personal reasons. Although the number of respondents endorsing the hiding of face or voice was not large, those respondents were consistent about the reasons for doing so.

The cited reasons for hiding one's location are presented in Table 3.27. Stalkers are the primary concern, but many viewers simply want to avoid people that they do not want to see. One person (who endorsed the concern for stalkers) also commented "I'm in the public eye and would prefer my location to be more vague".

Table 3.27 Endorsement of Options citing Reasons to Hide Location (GPS)

	<i>N</i>	%
Stalker	29	69.0
Avoiding People	21	50.0
Prevent Government tracking/monitoring	3	7.1
Prevent Employer tracking/monitoring	6	14.3
Social reason (being judged on locations)	10	23.8
Personal reasons (showing what I am doing)	6	14.3

Table 3.28 provides the correlations for hiding location.

Table 3.28 Correlations between Reasons to Hide Location.

	Being found	Governments	Professional reasons	Social reasons	Personal reasons
stalkers	<b>0.303</b>	0.004	0.146	-0.068	0.146
being found		-0.078	0.151	-0.084	0.283
governments			0.155	0.284	0.155
professional reasons				0.259	0.228
social reason					0.101

The average correlation was  $r = 0.132$  (SD: 0.134, min  $-0.084$ ; max 0.303). The mean absolute value was  $|r| = 0.163$ , which was small. There was only one significant correlation (stalkers and being found), and that was small.

### 3.2.7 Periscope Use

Because of the special properties of Periscope, there was a special section of the questionnaire devoted to Periscope. A total of 33 participants complete all or most of this section.

The first item of that section asked about the audience. Participants were asked, “How often do you broadcast privately to the following users?” and responses were collected as a five-point scale (“never” = 0, “rarely” = 1, “sometimes” = 2, “often” = 3, and “always” = 4) within the categories of “family members”, “offline friends”, “acquaintances”, “online only friends (people I have never met physically)” “people I follow (am a fan of)” and “people I work with”, with one open-ended option (“other”). Table 3.29 summarizes the data. Note that although 4 respondents indicated “other”, no one cited who those others might be. There were 8 respondents who did not indicate any audience (i.e., they were missing on all categories, though they did complete other later components of the Periscope section). In Table 3.29, the *N* under Any is the number who endorsed that type of audience, and the *N* under Exclusive is the number who only endorsed that type of audience. The percentage under Any is the percent of the sample of 33 respondents. The percentage under Exclusive is the percentage of the Any. That is, for Family contact, 4.8% of the 21 respondents only used Periscope to contact family. The level is the mean rating on the previous five-point scale.

Table 3.29 Audience Choice for Periscope Users

	Any		Exclusive		Frequency (Intensity of Use)			
	<i>N</i>	%	<i>N</i>	%	Mean	SD	Min	Max
Family	21	63.6	1	4.8	2.03	1.79	0	4
Friends Offline	24	72.7	2	8.3	1.67	1.34	0	4
Acquaintances	14	42.4	0	0.0	0.76	0.97	0	3
Friends Online	11	33.3	0	0.0	0.70	1.13	0	3
People I Follow	11	33.3	0	0.0	0.73	1.01	0	3
Work	11	33.3	0	0.0	0.64	1.03	0	4
Others	11	33.3	0	0.0	0.12	0.70	0	4

Family and Offline Friends, which have the highest levels of endorsement, is less of an issue for security. However, the other options have much lower levels of endorsement, but still sufficient for there to be concerns about privacy and security. Note that very few respondents use any one category exclusively.



In the previous part of the questionnaire, participants were asked, “Do you know that these apps do not enable the viewers to save the broadcasts?” Responses were collected as “yes”, “no” and “I know that Periscope allows one to save videos for up to 24hr (but the others do not).” Of the 33 respondents who completed the periscope section, 6.1% did not respond ( $N = 2$ ), 18.2% ( $N = 6$ ) said “no”, 36.4% ( $N = 12$ ) said “yes”, and 39.4% ( $N = 13$ ) claimed knowledge of Periscope. Respondents were also asked, “Do you know that these apps do not enable the viewers to replay the broadcasts?”, with similar options of “yes”, “no” and “I know that Periscope allows one to replay videos for up to 24hr (but the others do not).” Of the 33 respondents who completed the periscope section, 6.1% did not respond ( $N = 2$ ), 24.2% ( $N = 8$ ) said “no”, 33.3% ( $N = 11$ ) said “yes”, and 36.4% ( $N = 12$ ) claimed knowledge of Periscope. It would seem that 18 to 22% of the uses of Periscope have an incomplete knowledge of the capabilities of the app that they use.

With respect to the (temporary) saving of broadcasts, participants were asked “How often do you do the each of the following?” The options included “Keep the broadcast available for 24 hour”, “Keep the broadcast available for less than 24 hour”, “Delete the broadcast immediately” or “other”. Responses were collected on a five-point scale as “never” (0), “rarely” (1), “sometimes” (2), “often” (3), and “always” (4). Table 3.30 summarizes the results.

As above, in Table 3.29, the  $N$  under Any is the number who endorsed that type of retention, and the  $N$  under Exclusive is the number who only endorsed that type of retention. The percentage under Any is the percent of the sample of 33 respondents. The percentage under Exclusive is the percentage of the Any. That is, for 24 hour retention, 20.0% of the 25 respondents retained the broadcast for 24 hour. The level is the mean rating on the previous five-point scale.

Table 3.30 Retention Interval for Broadcasts

	Any		Exclusive		Frequency			
	<i>N</i>	%	<i>N</i>	%	Mean	SD	Min	Max
24 Hour	25	75.8	5	20.0	2.36	1.64	0	4
< 24 Hour	24	72.7	0	0.0	1.52	1.20	0	4
0 Hour (delete immediately)	25	75.8	3	12.0	1.48	1.30	0	4
Other	3	9.1	0	0.0	0.27	0.98	0	4

A substantial proportion of users retain the video for 24 hours (76%) at least some of the time, and 20% do so exclusively. Only 12% delete the video immediately. Three respondents cited other options, but only one specified that option as “Katch” (a utility to capture temporary broadcasts). Retaining a broadcast for longer periods is more of a privacy/security risk.

Participants were asked why they would keep the broadcast (“If you keep the broadcast available, why would you keep it available for replay?”). Responses were collected using a yes/no checklist with an open-ended option. No one provided any comments. Table 3.31 summarizes the results.

Table 3.31 Reasons to Keep a Video

	<i>N</i>	%
It can be useful	22	66.7
I like to review it	17	51.5
Viewer have requested it	7	21.2
I use it for content re-evaluation	13	39.4
I use it for self-evaluation	17	51.5
I want to know who the viewers are/were	15	45.5
I want to block viewers	6	18.2
I want to follow viewers	10	30.3
I want to obtain more feedback	17	51.5

There are a wide variety of cited reasons, and no one reason seems to dominate. On average,

respondents cited 3.75 (SD: 2.33) different reasons to keep a broadcast. However, the range was from none (no cited reasons) to 9.

Participants were asked why they would delete the broadcast (“If you delete the broadcast immediately, why would delete it immediately?”). Responses were collected using a yes/no checklist with an open-ended option. The comments included “I change my mind about broadcasting the video”, Sometimes I have my location on by mistake and delete the video.” and “not being totally prepared.”, none of which were recoded into the predefined categories. Table 3.32 summarizes the results.

Table 3.32 Reasons to Delete a Video

	<i>N</i>	%
Something embarrassing has been said about my physical appearance	8	24.2
There are inappropriately rude comments	14	42.4
There are inappropriate sexual comments	9	27.3
There are inappropriate comments or gossip	11	33.3
There are inappropriate or dangerous religious comments	8	24.2
There are inappropriate or dangerous political comments	9	27.3
I want to protect my privacy	22	66.7
I want to protect the privacy of others	14	42.4
I do not want it to fall into the wrong hands.	11	33.3

There are a wide variety of cited reasons, and no one reason seems to dominate. On average, respondents cited 3.21 (SD: 2.76) different reasons to keep a broadcast and the range was from none (no cited reasons) to 9.

Interestingly, the number of reasons to keep the broadcast was positively correlated with the number of reasons to delete the broadcast ( $r = 0.504, p < 0.003$ ) indicating that those respondents who see more pros also see more cons as well.

Periscope has the capacity to reveal the GPS location of the Broadcaster. Hence, participants were asked, “With respect to the show location feature of Periscope:”, with two options: know that Periscope shows my location (GPS) by default” and “I know that I can turn it

on and off”. Responses for both options were collected using a yes/no checklist. Of the 33 respondents, only 16.1% ( $N = 5$ ) knew of the default action (10 missing values) and only 19.4% ( $N = 6$ ) knew of the ability to change the default (10 missing values).

The propensity to reveal location while broadcast was asked with “How often do you reveal your location?”. There were two options: “While driving” and “While creating other broadcasts” (generally) and responses were collected using a five-point scale as “never” (0), “rarely” (1), “sometimes” (2), “often” (3), and “always” (4). Table 3.33 summarizes:

Table 3.33 Revealing Location

	Any		Exclusive		Frequency			
	<i>N</i>	%	<i>N</i>	%	Mean	SD	Min	Max
Generally (not driving)	15	45.5	6	40.0	0.26	0.45	0	1
While Driving	9	27.3	0	0.0	0.22	0.42	0	1

In Table 3.32, the  $N$  under Any is the number who endorsed that type of location at any level greater than never, and the  $N$  under Exclusive is the number who only endorsed that type of location revealing. The percentage under Any is the percent of the sample of 33 respondents. The percentage under Exclusive is the percentage of the Any. The level is the mean rating (of frequency) on the previous five-point scale. About half of the Periscope users reveal their location while driving.

Participants were asked what for the benefits of the location revealing feature using, “What are the potential benefits of revealing your location while broadcasting (i.e., GPS)?”. Responses were collected using a yes/no checklist with an open-ended option. There were two comments “I’m from SA and enjoy watching scopes from my home” and “Just to get views”. Table 3.34 summarizes the results.

Table 3.34 Benefits for Revealing Location

	<i>N</i>	%
Finding people in an emergency	14	42.4
Tracking people to ensure they are OK	9	27.3
Parents can track their children	14	42.4
Providing directions to friends and family	9	27.3
Tracking loved ones to surprise them	11	33.3
The comfort of remote awareness of friends and family	2	6.1
So people can find me	10	30.3
Tracking my own activities	5	15.2

There are a wide variety of cited reasons, and no one reason seems to dominate. On average, respondents cited 2.24 (SD: 1.87) different reasons to keep a broadcast. However, the range was from none (no cited reasons) to 8.

Participants were asked about the potential risks for revealing location with “What are the potential risks of revealing your location while broadcasting (i.e., GPS)?”. Responses were collected using a yes/no checklist with an open-ended option. No one provided any comments. Table 3.35 summarizes the results.

Table 3.35 Risks for Revealing Location

	<i>N</i>	%
Revealing the location of my home	23	69.7
Being found by someone I do not want to see	25	75.8
Being found when I want to be alone	15	45.5
Revealing activities I am involved in	8	24.2
Being judged on the locations I visit	10	30.3
Being stalked (e.g., sexual predators)	14	42.4
Enabling government to track or monitor me	5	15.2
Enabling employers to track me	6	18.2

There are a wide variety of cited reasons, and no one reason seems to dominate. On average, respondents cited 3.21 (SD: 1.71) different reasons to keep a broadcast. However, the range was from none (no cited reasons) to 8.

The number of benefits was positively correlated with the number of risks ( $r = 0.472$ ,  $p < 0.006$ ) implying that respondents see a number of pros and cons for revealing location — and those who see more benefits also see more risks.

### **3.2.8 Relationships between Variables**

The analysis of the main questionnaire contained 108 separate items, classified within several groups: Demographics (5 items), Apps Used (4 items; Table 3.1), Reasons for Use (11, expanded to 13 items; Table 3.3), Category of Broadcast (5 items; Table 3.5), Broadcast Audience (4 expanded to 5 items; Table 3.7), Broadcast Planning (2 expanded to 3 items; Table 3.8), Broadcast Location (5 items; Table 3.9), Broadcast Mood 1 (6 items; Table 3.11), Broadcast Mood 2 (7 items, Table 3.12), Limitations on Use (6 items; Table 3.14), Knowledge of Temporary Nature (2 items) Concerns (9 items; Table 3.15), Positive Aspects of the Temporary Nature (9 items; Table 3.17), Negative Aspects of the Temporary Nature (6 items; Table 3.19), Desired Feedback (4 items; Table 3.21), Attributes to Hide (8 items; Table 3.23), Reasons to Hide Face (5 items; Table 3.25), Reasons to Hide Voice (5 items; Table 3.25), and Reasons to Hide Location (6 items; Table 3.27). This list does not include the fact that Broadcast Audience, Planning, Location, and Mood 1 were each considered within five different Types of broadcast (Formal Self, Informal Self, Formal Other, Informal Other, and Other Non-Human) — a further 72 items. This also does not include the section of the questionnaire that was devoted to Periscope.

Clearly, it is not practical to examine the relationships between all variables as that would entail the examination and discussion of 5778 (or 16110 considering the 5 Types of broadcast) separate associations (e.g., correlations for continuous variables; phi-correlations ( $\Phi$ ), t-tests, or ANOVAs for categorical variables). That does not consider more complex multi-variate relationships. Hence, the goal of the current section is to consider the conceptually important relationships. The focus of the current work is the security and privacy issues associated with the use of live video broadcasting applications (LVBAs) that do not create (store) permanent

materials on the Internet (temporal-content social media).

### Demographics

The relationships between the demographic variables are provided in Table 3.36. Age and Education were coded in ranges (ordinal scale). Comfort was a self-assessment using a six-point ordinal scale with higher values implying *less* comfort. Knowledge of security was using a three-point ordinal scale with higher values implying *more* knowledge. This analysis is based on the 43 respondents who provided answers to all items.

Table 3.36 Correlation between Demographic Measures.

	Age Group	Education Group	Comfort with Technology	Knowledge of Security
Sex	-0.010	<b>0.310</b>	-0.012	0.088
Age Group		<b><i>0.528</i></b>	<b>0.387</b>	0.035
Education Group			0.233	0.146
Comfort with Technology				-0.256

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  or  $43$  for all comparisons.

Note that there is an expected relationship between Age and Education. There is a relationship between Sex and Education (males higher), which is not surprising given the international scope of the study. There is also a relationship between Age and Self-Reported Comfort with Technology, in that older individuals are *less* comfortable. This may be due, in part, to education and comfort (which did not reach significance). Note that the correlations for Age and Education with Comfort are similar. There is a negative (though non-significant) correlation between Comfort and Knowledge, which is reasonable given the scaling of the variables: higher Comfort is associated with higher Security. It should be added that the highest correlation of  $r = 0.538$  only implies  $r^2 = 0.279$ , or 27.9% overlap. This implies that further analyses involving these demographics should consider all (i.e., cannot discard any).

### *App Group*

AppGrp was coded as a single variable with 5 levels: 1: Periscope exclusive, 2: YouNow exclusive, 3: Meerkat exclusive, 4: Other exclusive, and 5: Multiple (non-exclusive use). AppGrp was coded as the maximum level of use in any one category.

Differences between use as a function of group were tested with each “important” variable. The goal was to determine whether or not subsequent analysis had to consider each app (e.g., Periscope, YouNow, Meerkat, Other, Multiple) in isolation. That is, it is more efficient to analyze all the apps as one large group, but since apps have different capabilities (particularly Periscope), they may attract different users, may be used in different ways, or many have different issues.

### *Apps Used Summary*

What follows is the long, detailed, analysis of app use. However, to spare the reader, in summary (as would be used in a short publication) Demographics, Reasons for Use, Categories of Use (broadcasts), Privacy, Planning, Location, Mood, Restrictions on Use, Concerns, and cited Positive or Negative aspects of the Temporal Nature of broadcasts, did *not* differ significantly as a function of the app used (i.e., AppGrp). All apps are basically used in the same way, with the same concerns and issues. There were minor (significant) differences on the occasional measures, but by and large, it is reasonable to combine all participants — regardless of app(s) used — into a single group. On the one hand, given that the apps are functionally quite similar, this is not too surprising. On the other hand, given that Periscope has somewhat distinct capabilities, this is a bit surprising. Combining participants into one group provides greater statistical power and more confidence in the generalizations to the population (i.e., a larger sample size is a better basis for inferences).

### *App Group and Demographics*

Table 3.37 presents the group differences (AppGrp) on demographics.



Table 3.37 Means and Analysis of Group Differences for Sex, Age, Education, Comfort with Technology, Knowledge of Security

	Periscope	YouNow	Meerkat	Other	Multiple	<i>F</i>	<i>p</i> ( <i>F</i> )	$\eta^2$
N (Sample size)	16	6	7	2	13			
Sex	1.31	1.83	1.43	1.00	1.46	1.671	0.176	0.146
Age Group	1.94	1.17	2.57	1.50	1.85	2.219	0.085	0.185
Education Group	3.38	2.50	3.57	3.50	3.58	0.727	0.579	0.071
Comfort Technology	1.40	1.33	2.29	2.00	1.67	1.705	0.170	0.156
Knowledge Security	1.19	1.67	1.29	1.50	1.23	0.374	0.826	0.037

Notes:  $df=(4,39)$  for all except Comfort with Tech for which  $df=(4,37)$ ;

Sex was coded as 1 for female, and 2 for male.

There were no group differences on any of these variables. That is, all groups were basically equivalent. Post hoc testing using a Bonnferroni correction for type 1 error rate with  $\alpha / 10 = 0.005$  ( $\alpha$  divided by the number of tests conducted for *each* DV) did not find any significant differences; when using an uncorrected type one error rate of  $\alpha = 0.05$ , there were 10 differences for a total of 60. The effect sizes ranged from 0.04 to 0.19, which are in the small range.

Note that an ANOVA for a DV that is dichotomy is functionally equivalent to (but not *identical* with) the Pearson Chi-Square. For example, for Sex by AppGrp  $\chi^2(4) = 6.438$  ( $p < 0.169$ ). Similarly, the non-parametric Kruskal-Wallis for Age group produces  $\chi^2(4) = 8.039$  ( $p < 0.090$ ), and for Education group produces  $\chi^2(4) = 2.711$  ( $p < 0.601$ ). Note that the  $p$ -values (the only statistic that really matters) are very similar to that of the ANOVA (addendum: one should always view any  $p \approx 0.05$  — one that it close to the criterion — with caution; many advocate “suspend judgment”).

Finally, it should be noted that the Other group has only 2 participants. However, excluding this group had minimal impact on the results (the  $p$ -values were similar and the interpretations unchanged). The ANOVA is a weighted analysis such that the impact of any particular group mean on the outcome is weighted by the sample size. Hence, means from small groups do not exert much influence on the analysis. Nonetheless, in the subsequent analyses, the small Other group is ignored (though the descriptive statistics are reported)

*App Group and Reasons for Use*

Table 3.38 shows that the Reasons for Use did not differ markedly by AppGrp.

Table 3.38 Percent Endorsement by Group (AppGrp) for Reasons for Use.

	Periscope	YouNow	Meerkat	Other	Multiple	<i>F</i>	<i>p(F)</i>	$\eta^2$
N (Sample size)	16	6	7	2	13	(3,38)		
Friends Online	43.8	83.3	42.9	0.0	30.8	1.575	0.211	0.111
Friends Offline	12.5	16.7	0.0	100.0	7.7	0.407	0.749	0.031
Strangers	12.5	16.7	0.0	0.0	15.4	0.383	0.766	0.029
Find New Friends	37.5	66.7	57.1	0.0	30.8	0.952	0.425	0.070
Find New Followers	12.5	16.7	42.9	0.0	46.2	1.755	0.172	0.122
Advocate for Change	6.3	0.0	0.0	0.0	23.1	1.459	0.241	0.103
Offer Help	12.5	16.7	28.6	0.0	15.4	0.287	0.835	0.022
Provide Advice	6.3	16.7	14.3	0.0	0.0	0.532	0.663	0.040
Self Promote: Professional	12.5	16.7	0.0	0.0	23.1	0.652	0.587	0.049
Self Promote: Business	12.5	0.0	0.0	0.0	30.8	1.748	0.174	0.121
Self Promote: Events	0.0	0.0	0.0	0.0	15.4	1.590	0.208	0.111
Entertainment	12.5	0.0	14.3	50.0	0.0	0.868	0.466	0.064

Notes: *df*=(3,38) for all

Note that the reported analyses do not include the other group. If the other group is included, the basic results are the same (i.e., accept/reject).

*App Group and Categories of Use*

The Categories of Use data were collected in five categories Formal broadcasts of Self, Informal broadcasts of Self, Formal broadcasts of Others, Informal broadcasts of Others and Non-Human broadcasts along the dimensions of Audience Type, Planning, Location, and Associated Emotion. Any use within the five categories was coded in a binary (dichotomous) fashion.

Table 3.39 presents the percent endorsement of each Category of Use (see Table 3.5) as a

function of group.

Table 3.39 Category of Use by AppGrp

	Periscope	YouNow	Meerkat	Other	Multiple	<i>F</i>	<i>p</i> ( <i>F</i> )	$\eta^2$
N (Sample size)	16	6	7	2	13	(4,39)		
Formal broadcasts of Self	75.0	83.3	28.6	0.0	76.9	2.354	0.087	0.157
Informal broadcasts of Self	75.0	100.0	85.7	50.0	76.9	0.640	0.594	0.048
Formal BsC of Others	56.3	83.3	14.3	50.0	76.9	3.485	0.025	0.216
Informal broadcasts of Others	50.0	100.0	57.1	50.0	76.9	2.071	0.120	0.140
Non-Human broadcasts	56.3	66.7	14.3	0.0	61.5	1.749	0.173	0.121

Notes:  $df=(3,38)$  for all

Because the categories were so highly correlated (see Table 3.6), a mixed ANOVA with one within-subjects factor (Category) and one between-subjects factor (AppGrp) was conducted first. There was no main effect of Category with  $F(4,42) = 1.746$  ( $p < 0.142$ ,  $\eta^2 = 0.040$ ), no main effect of AppGrp with  $F(4,42) = 0.068$  ( $p < 0.795$ ,  $\eta^2 = 0.002$ ), and no interaction between Category and AppGrp with  $F(4,42) = 0.762$  ( $p < 0.551$ ,  $\eta^2 = 0.018$ ). Note that the effect sizes (the  $\eta^2$ ) are small (less than 5%). The important message is that the Category of Use does not differ by group (the lack of an interaction) and that the different categories of use all have about the same amount of endorsement (the lack of a main effect category). Also note that the main effect of AppGrp is not a test of the difference between the numbers of users. It is a test of whether the mean amount of endorsement *collapsed across Categories* differs as a function of group.

For simplicity, Table 3.39 presents the simple-effects analysis within each individual level of Category, ignoring the Other group (due to its small sample size). This reaffirms the lack of effects. The basis message is that the apps are used in a similar way.

### *App Group and Privacy*

Collapsed over Categories (i.e., Formal or Informal broadcasts of Self or Others; Non-Human broadcasts) type of audience was coded as Exclusively Private, Exclusively Public or Both (see Table 3.7). Because Audience type is a three-level categorical variable (i.e., each respondent falls into just one category), the analysis of the relationship between Audience type and AppGrp was a two-way Chi-Square. Table 3.40 presents the data.

Table 3.40 Percentage of Respondents Endorsing each level of Audience Type by AppGrp.

Audience Type	Periscope	YouNow	Meerkat	Other	Multiple	Total
N (sample size)	16	6	7	2	13	44
Private	12.5	33.3	28.6	100.0	46.2	31.8
Public	50.0	16.7	14.3	0.0	23.1	29.5
Both	18.8	33.3	42.9	0.0	15.4	22.7
NA	18.8	16.7	14.3	0.0	15.4	15.9

The  $\chi^2(df=6) = 11.426$  ( $p < 0.178$ ) implied that the pattern of Audience type did *not* differ as a function of AppGrp. Excluding the Other group, the analysis was still not significant with  $\chi^2(df=8) = 8.538$ ,  $p < 0.201$ . Note that the NA group did not provide the Audience type, so it was not considered in either analysis.

Overall, about 32% used the apps exclusively privately, 30% used the apps exclusively publically, and 23% used the apps for both. This implies that 70% are engaged in public broadcasting (exclusive or mixed) with its associated security risks.

### *App Group and Planning*

Collapsed over Categories (i.e., Formal or Informal broadcasts of Self or Others; non-human broadcast), there was the degree of planning which was simply coded as Exclusively Planned, Exclusively Spontaneous or Both (see Table 3.8). Because Planning is a three-level categorical variable (i.e., each respondent falls into just one category), a Chi-Square analysis is used. Table 3.41 presents the two-way Chi-Square analysis of the relationship between Planning and

AppGrp.

Table 3.41 Percentage of Respondents Endorsing each level of Planning by AppGrp.

Planning Level	Periscope	YouNow	Meerkat	Other	Multiple	Total
N (sample size)	16	6	7	2	13	44
Planned	12.5	0.0	0.0	0.0	0.0	4.5
Spontaneous	18.8	0.0	14.3	0.0	15.4	13.6
Both	62.5	83.3	85.7	100.0	69.2	72.7
NA	6.3	16.7	0.0	0.0	15.4	9.1

The  $\chi^2(df=8) = 5.426$  ( $p < 0.711$ ) implied that the pattern of Planning did *not* differ as a function of AppGrp. Excluding the Other group, analysis was still not significant with  $\chi^2(df=6) = 5.209$ ,  $p < 0.517$ . The NA group was not included in either analysis.

Overall, about 4.5% used the apps exclusively planned, 14% used the apps exclusively spontaneously, and 73% used the apps planned or spontaneously. This further implies that some 95% are engaging in spontaneous broadcasting with its heightened security risks.

### *App Group and Location*

Collapsed over Categories (i.e., Formal or Informal broadcasts of Self or Others; Non-Human broadcasts) the location of broadcasting was dichotomously coded within five levels (see Table 3.9): Work, Home, Public, Parties or Driving. Respondents could endorse as many locations as desired, but in fact, most respondents only indicated a single location per Category of broadcast. Collapsed across Categories, the correlations were weak. As such, each location can be analyzed in isolation. Table 3.42 presents the ANOVA for each location as a function of the five types of app.

Table 3.42 Location by AppGrp

	Periscope	YouNow	Meerkat	Other	Multiple	<i>F</i>	<i>p(F)</i>	$\eta^2$
N (Sample size)	16	6	7	2	13	(3,38)		
Work	56.3	50.0	14.3	50.0	23.1	1.918	0.143	0.131
Home	81.3	83.3	57.1	100.0	76.9	0.567	0.640	0.043
Public	75.0	50.0	57.1	50.0	69.2	0.493	0.689	0.038
Parties	31.3	33.3	42.9	50.0	46.2	0.246	0.863	0.019
Driving	18.8	33.3	42.9	50.0	15.4	0.779	0.513	0.058

The analyses did not include the Other group (due to the small sample size; power in the ANOVA is related to the average sample size, so including a small group reduces the overall ability to detect differences - this group is eliminated from all similar analyses). Note that there are no significant differences and the effect sizes ( $\eta^2$ ) are quite small. The effect size for broadcast at work is the largest, and imply that Meerkat is not used at work. The location of the broadcast is not related to the app used which is an important point because some apps provide the broadcaster’s GPS location by default.

*App Group and Mood*

Mood while broadcasting was collected for each category of broadcast (see Table 3.11). Mood was also collected “overall” (see Table 3.12) using a five-point Likert scale as frequency of occurrence while broadcasting. The pattern overall resembled the pattern within each category. Hence, herein, the overall mood was analyzed as a function of app use. Note that driving was included in the overall because of the particular implications when combined with stimulants.

Previous analyses (see Table 3.13) indicated that the moods were not completely independent (e.g., Worried, Sad and Angry were all correlated: Angry and Stims were correlated). However, it is possible to analyze each mood in isolation as long as one realizes that the analyses of Sad, Angry and Worried are somewhat redundant (even then the overlap is, at most, 21.5%)

Table 3.43 presents the ANOVA for each mood as a function of the five types of app.

Table 3.43 Mood by AppGrp

	Periscope	YouNow	Meerkat	Other	Multiple	<i>F</i>	<i>p(F)</i>	$\eta^2$
N (Sample size)	16	5	7	2	12	(3,36)		
Happy	3.00	3.20	3.71	2.00	2.92	0.898	0.452	0.070
Sad	0.38	0.20	1.29	0.00	0.75	2.549	0.071	0.175
Angry	0.38	1.20	1.00	0.00	1.08	1.769	0.171	0.128
Worried	0.56	0.20	1.86	0.50	1.08	4.093	0.013	0.254
Stimulants	0.00	0.00	0.43	0.00	0.50	3.113	0.038	0.206
Compelled	2.25	1.20	2.14	0.50	1.67	0.701	0.558	0.055
Driving	1.00	0.80	0.86	0.00	0.50	0.314	0.815	0.025

As always, the actual analysis does not include the Other group (due to small size). The only moods that were different were Worried and Stimulants, which have a higher frequency for the Meerkat app. As would be expected from the correlations, Sad was also somewhat elevated for the Meerkat app (but differences were not significant). In fact, all moods for Meerkat were generally reported as higher across the board, even Happy, which might seem to contradict Worried and Sad. It may be that these seven respondents simply exhibit elevated mood across the board (the effect is not caused by a single respondent). Note that, across all apps, the mean frequency for Stimulants and for Driving is quite low.

*App Group and Restrictions on Use*

Collapsed over Categories, Restrictions on Use were collected as six dichotomies (see Tables 3.15). Table 3.44 presents the level of endorsement for each app and the associated ANOVA.

Table 3.44 Restrictions by AppGrp

	Periscope	YouNow	Meerkat	Other	Multiple	<i>F</i>	<i>p(F)</i>	$\eta^2$
N (Sample size)	16	6	7	2	13			
Not Restricted	56.3	50.0	85.7	50.0	53.9	0.789	0.507	0.059
Restricted								
By Lack of Content	18.8	0.0	0.0	50.0	7.7	0.974	0.415	0.071
By Lack of time	6.3	50.0	14.3	0.0	23.1	1.976	0.134	0.135
By data plan	25.0	0.0	0.0	0.0	23.1	1.254	0.304	0.090
By costs	6.3	0.0	0.0	0.0	0.0	0.523	0.669	0.040
By security	12.5	16.7	0.0	0.0	15.4	0.383	0.766	.029

The analysis does not include the Other group (due to small size). There were no significant differences and the effect sizes ( $\eta^2$ ) are quite small.

*App Group and Knowledge of Saving/Replaying the broadcast*

Respondents were asked if they knew that the apps did *not* save broadcasts and if they knew that the apps did not allow for re-broadcasting. There were three possible options: No, “Yes” and “Knowledge of Periscope”. The responses were categorical different (and mutually exclusive), so the analysis of the relationship is a two-way  $\chi^2$ . Tables 3.45 and 3.46 present the data for each.

Table 3.45 Percentage of Respondents Endorsing Each Level of Knowledge about Saving by AppGrp.

Knowledge of broadcast Saving	Periscope	YouNow	Meerkat	Other	Multiple	Total
N (sample size)	16	5	7	2	10	40
No	0.0	40.0	28.6	50.0	40.0	22.5
Yes	37.5	40.0	71.4	50.0	30.0	42.5
Knows of Periscope	62.5	20.0	0.0	0.0	30.0	35.0



Table 3.46 Percentage of Respondents Endorsing each level of Knowledge about Re-Broadcasting by AppGrp.

Knowledge of broadcast Re-Broadcasting	Periscope	YouNow	Meerkat	Other	Multiple	Total
N (sample size)	15	5	7	2	11	40
No	13.3	20.0	28.6	50.0	45.5	27.5
Yes	20.0	80.0	71.4	50.0	36.4	42.5
Knows of Periscope	66.7	0.0	0.0	0.0	18.2	30.0

More users of Periscope have specific knowledge about Periscope, but even still about 1/3 of Periscope users were not aware of the fact that Periscope can save broadcasts. More generally, about 1/4 of all respondents did not know that the apps do not save broadcasts.

Knowledge of Saving differed across groups with  $\chi^2(df=6) = 13.928 (p < 0.0005)$ .

Knowledge of Re-broadcasting differed across groups with  $\chi^2(df=6) = 17.805 (p < 0.0005)$ .

Knowledge of saving and knowledge or re-broadcasting were highly related as shown in Table 3.47.

Table 3.47 Percentage of Respondents Endorsing each level of Knowledge about Saving and about Re-Broadcasting

		Knowledge of Saving			Totals
		No	Yes	Knows of periscope	
Knowledge of Re-Broadcasting	No	7	2	2	11
	Yes	2	13	1	16
	Knows or periscope	0	1	11	12
Totals		9	16	14	39

The  $\chi^2(df=6) = 37.480, p < 0.0005$  and the Kappa = 0.687 ( $p < 0.0005$ ). That is, the two variables essentially tap the same structure (most respondents fall along the diagonal of Table 3.46).

### App Group and Concerns

Concerns were collected in 9 categories (see Table 3.15). Previous analyses indicated that they could be grouped, but the individual categories were retained for the current analysis because “concerns” is a main focus of the current work. Table 3.48 presents the means of each concern per AppGrp.

Table 3.48 Ratings of Concerns by AppGrp.

	Periscope	YouNow	Meerkat	Other	Multi	<i>F</i>	<i>p</i> ( <i>F</i> )	$\eta^2$
	16	5	7	2	11			
Social	2.13	1.60	2.29	0.50	2.09	0.552	0.650	0.045
Physical	1.88	2.00	2.00	2.50	2.18	0.214	0.886	0.018
Economic	2.06	1.40	1.71	1.50	1.55	0.610	0.613	0.050
Unauthorized Use	1.38	1.80	1.57	2.50	1.45	0.251	0.860	0.021
ScreenShot Theft	2.06	1.00	2.00	1.50	1.64	1.518	0.227	0.115
Controlling Viewers	1.88	1.80	1.29	2.50	1.64	0.924	0.439	0.073
Controlling Location	2.31	2.40	1.57	1.00	2.36	1.764	0.172	0.131
Viewers								
Lawsuits	1.25	0.60	1.00	2.00	1.45	1.062	0.377	0.083
Employers	1.31	0.80	1.57	0.50	1.55	1.085	0.368	0.085

Because the Concerns were moderately correlated (see Table 3.16), the full analysis of Concerns by AppGrp is a mixed ANOVA with one within-subjects factor (Concern) and one between subjects factor (AppGrp). That analysis indicated a significant main effect of Concerns with  $F(8,280)=5.448$  ( $p < 0.0005$ ,  $\eta^2 = 0.135$ ), *no* main effect of AppGrp with  $F(3,35)=0.529$  ( $p < 0.666$ ,  $\eta^2 = 0.043$ ), and *no* interaction between Concerns and AppGrp with  $F(8,280)=5.448$  ( $p < 0.0005$ ,  $\eta^2 = 0.135$ ). The main effect of Concerns is essentially the same effect as reported previously with Tables 3.15. The lack of a main effect of AppGrp implies that all respondents — regardless of the app used — have about the same level of overall concern. The critical lack of a main effect of the interaction shows that the relative ranking of concerns is the *same* for the different apps. As such, Table 3.48 presents the simple effects analysis for each concern as a

function of AppGrp.

*App Group and Temporary Nature of the broadcast*

Respondents were asked, using a number of checklists, whether or not the temporary nature of the broadcast was a good thing, or a bad thing. Table 3.49 presents the details for both. All analyses did not include the Other group (though the data is presented).

Table 3.49 Percentage of Respondents Endorsing the Good and Bad Features of the Temporary Nature of Broadcast, by AppGrp.

	Periscope	YouNow	Meerkat	Other	Multiple	<i>F</i>	<i>p(F)</i>	$\eta^2$
	16	6	7	2	13			
<b>Good</b>								
keeps contents secretive	18.8	33.3	57.1	0.0	15.4	1.662	0.191	0.116
protects my privacy	50.0	66.7	57.1	50.0	53.8	0.156	0.925	0.012
protects my intellectual property	18.8	16.7	0.0	0.0	7.7	0.637	0.596	0.048
reduces unwanted viewers	37.5	16.7	0.0	0.0	53.8	2.463	0.077	0.163
enables people to forget me	0.0	33.3	42.9	0.0	0.0	5.641	0.003	0.308
prevent people from profiling me.	37.5	16.7	14.3	0.0	30.8	0.558	0.646	0.042
minimizes data companies collect about me	25.0	16.7	0.0	50.0	7.7	1.029	0.391	0.075
protects privacy of others	37.5	33.3	0.0	0.0	15.4	1.577	0.211	0.111
minimizes data companies collect about others	25.0	16.7	0.0	50.0	7.7	1.029	0.391	0.075
<b>Bad</b>								
content could be valuable.	68.8	16.7	85.7	50.0	23.1	5.220	0.004	0.292
cannot know who watched broadcast	50.0	50.0	14.3	0.0	38.5	0.920	0.441	0.068
reduces number of viewers	37.5	0.0	14.3	50.0	30.8	1.275	0.297	0.092
need to recreate for each broadcast	18.8	16.7	0.0	0.0	38.5	1.444	0.245	0.102
enables people to forget me	6.3	33.3	0.0	0.0	15.4	1.411	0.254	0.100
limits potential popularity of broadcast	25.0	33.3	0.0	0.0	15.4	0.947	0.428	0.070

Firstly, most of the reasons did not differ significantly across groups. However, AppGrp is related to the good feature of enabling people to forget the broadcaster, such that this option is

not endorsed by Periscope users and is endorsed by Meerkat users. AppGrp is related to the “bad” feature that the content could be valuable: Periscope and Meerkat users are more concerned about that, but Meerkat more so than Periscope.

### *Reasons for Use*

The previous analyses relating AppGrp to other variables demonstrated that the particular app used is, for the most part, unrelated to any particular aspects of use. As such, it is reasonable to combine all AppGrp groups (i.e., all respondents) into one group for subsequent analyses.

The associations were computed between the Reasons for Use and each of Concerns, Positive Features, Negative Features, Sensitive Information and Reasons to Hide Face, Voice or Location. The problem here is the number of associations. There are 12 Reasons for Use and 9 Concerns. Hence, there are 108 potential associations. There are 12 Reasons for Use and 9 Positive Features of the Ephemeral Nature of broadcasts. Again, there are 108 potential associations. There are 12 Reasons for Use and 6 Negative Features of the Ephemeral Nature of broadcasts or 72 potential associations. There are 12 Reasons for Use and 7 attributes of Sensitive Information or 84 associations. There are 12 Reasons for Use and 5 Reasons to Hide Face or Voice (60 associations each) and 6 Reasons to Hide Location (72 associations)

Each Reason for Use is a dichotomy (binary Yes/No). As such, one can use Reason as a grouping variable to define two groups: those who do not cite that reason vs those who do cite that reason. A two-group ANOVA (to two-group t-test) could be used to analyze Concerns as a function of each reason. A Chi-Square test can be used to analyze Positive Features, Negative Features, Sensitive Information and Reasons to Hide Face, Voice or Location as a function of each reason. A correlation can be used for all analyses, which enhances comparisons. The Pearson correlation is identical with the two-group t-test (the  $p$ -value is the same) and the two-group t-test is identical to the two-group ANOVA, although the presentation is different. The t-test emphasizes group differences whereas the correlation emphasizes the relationship). The phi-correlation ( $\Phi$ ) is the same as the Chi-Square test, and the Phi-correlation ( $\Phi$ ) is the same as Pearson correlation, though the presentation is slightly different (the 2x2 chi-square emphasizes percentage agreement, whereas the phi-correlation ( $\Phi$ ) emphasizes relationships). Herein, correlations are presented because they emphasize the relationships, are comparable across

analyses, and provide a more compact presentation.

*Reasons for Use & Concerns*

The associations between the Reasons for Use and the types of Concerns are presented in Table 3.50, which also includes the mean level of concern (from Table 3.15) as a baseline for comparison.

Table 3.50 Reasons for Use and Types of Concerns.

	Social	Physical	Economic	Unauthorized Use	ScreenShot Theft	Controlling Viewers	Controlling Location Viewers	Lawsuits	Employers
Concern Mean	2.00	2.02	1.76	1.54	1.78	1.73	2.15	1.22	1.32
Friends Online	0.000	0.246	0.093	<b>0.353</b>	0.219	-0.027	0.089	-0.299	-0.023
Friends Offline	<b>-0.358</b>	-0.011	0.028	<b>0.342</b>	-0.044	0.226	-0.154	0.122	-0.074
Strangers	-0.155	0.152	0.080	0.102	0.146	0.125	0.024	-0.086	-0.052
Find New Friends	<b>0.411</b>	-0.183	0.180	<b>-0.417</b>	-0.012	0.035	0.206	<b>0.327</b>	0.272
Find New Followers	0.229	0.222	0.033	0.063	0.176	-0.141	-0.170	0.092	0.165
Advocate for Chg	0.085	-0.009	0.070	-0.098	-0.240	-0.199	0.138	0.011	-0.124
Offer Help	-0.202	0.058	-0.300	-0.118	-0.270	-0.173	-0.079	0.100	0.138
Provide Advice	0.000	0.071	0.014	0.179	0.146	-0.155	-0.065	0.149	0.214
Promote: Profession	-0.171	0.080	0.286	0.158	-0.086	-0.096	0.138	-0.249	-0.124
Promote: Business	0.000	0.152	0.210	0.024	-0.132	-0.249	0.024	-0.086	-0.141
Entertainment	-0.256	-0.098	-0.218	-0.012	<b>-0.316</b>	-0.096	-0.252	0.011	<b>-0.320</b>

Notes: Total sample size was 41.

**Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ; N = 44 for all comparisons.

These are equivalent to point-biserial correlations, or to two-group t-tests.

The first observation is that the correlations tend to be small. The average correlation is only  $r = 0.001$  (SD: 0.177, min -0.417, max: 0.411), and the average of the absolute values is only  $|r| = 0.145$ . Only 8 were significant out of a total of 99. If the correlation is near zero (not significant),

then it is implied that those who do not cite that reason have the same level of concern as those who do cite that reason: Both groups are the same as the overall average. If the correlation is not near zero (e.g., is significant), then there is a relationship. A positive correlation implies that those who cite the reason have a higher level of concern than those who do not. A negative correlation implies that those who cite the reason have a lower concern than those who do not.. In either case, one group would be above the average and the other below (the actual means will depend on sample sizes as well).

There were 8 significant relationships. Recall that concerns four-point scale from 0 (“Never thought about it”) through 1 (“Not at all Concerned”), 2 “Concerned”, to 3 (“Very Concerned”). The highest correlation involved using broadcasts to Find New Friends. Those who use the broadcast for that purpose are more concerned about Social Harm (means: 1.67 vs. 2.47) and about Lawsuits (means: 0.96 vs. 1.59), but they are *less* concerned about Unauthorized Use of the broadcast (means: 1.88 vs. 1.06). In some sense, this is reasonable because if broadcasts are used to find friends, then the point is broad dissemination and as such, unauthorized use becomes irrelevant. However, there is always risk to self-exposure. Furthermore, it would seem that these individuals are concerned about their social world (the need to find friends) and as such, would be most concerned about the risks to that social world.

Those who used broadcast to maintain online or offline relationships were more concerned about the Unauthorized use of broadcasts (means online: 1.25 vs. 1.94; means offline: 1.40 vs. 2.33). However, the Offline group was much *less* concerned about Social Harm (means: 2.14 vs. 1.17).

Finally, those who use broadcasts for Entertainment are less concerned about the use of Screenshots (means 1.89 vs. 0.75), and less concerned about Monitoring by Employers (means: 1.41 vs. 0.50).

### *Reasons for Use & Positive Features Associated with the Temporary Nature of the broadcasts*

The associations between the Reasons for Use and the Positive Features Associated with the Temporary Nature of the broadcast are presented in Table 3.51, which also includes the mean percentage endorsement of each feature as a baseline for comparison (from Table 3.17).

Table 3.51 Reasons for Use and Positive Features of the Temporary Nature.

	Keep contents secretive	Protect my privacy	Protect intellectual property	Reduces unwanted viewers	enables people to forget me	prevent people from profiling me.	minimizes data companies collect about me	protects privacy of others	minimizes data companies collect: others
Mean Endorsement	26.2	57.1	11.9	33.3	11.9	28.6	16.7	23.8	16.7
Friends Online	0.026	-0.126	0.122	0.193	-0.023	<b><i>0.393</i></b>	0.248	<b><i>0.403</i></b>	0.248
Friends Offline	-0.229	0.097	-0.142	0.155	0.066	-0.095	0.189	-0.057	0.189
Strangers	0.124	0.183	0.097	0.063	0.097	0.102	0.236	0.148	-0.156
Find New Friends	0.053	0.295	0.139	0.027	0.285	0.009	-0.236	<b><i>-0.341</i></b>	-0.236
Find New Followers	<b><i>0.354</i></b>	0.149	0.102	0.020	0.263	0.083	0.292	0.155	0.013
Advocate for Chg	-0.183	-0.029	-0.113	0.123	-0.113	-0.016	-0.138	-0.171	-0.138
Offer Help	-0.251	-0.102	0.040	-0.164	0.040	-0.127	-0.189	-0.236	-0.189
Provide Advice	-0.076	-0.302	0.066	0.155	-0.142	0.203	0.008	0.101	0.189
Promote: Profession	-0.229	-0.169	0.066	-0.129	0.066	0.203	-0.173	-0.057	0.008
Promote: Business	-0.229	-0.169	0.275	0.013	-0.142	0.054	0.008	-0.057	0.008
Promote: Events	-0.126	-0.239	-0.078	-0.149	-0.078	0.111	-0.095	-0.118	0.203
Entertainment	0.000	<b><i>-0.346</i></b>	-0.113	0.123	-0.113	-0.194	-0.138	0.017	0.295

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ; N = 44 for all comparisons.

These are equivalent to phi-correlations, which are equivalent to chi-square analyses ( $\Phi = \sqrt{\chi^2 / N}$ )

As with the previous, the correlations tend to be small. The average correlation is only  $r = 0.001$  (SD: 0.169, min -0.346, max: 0.403), and the average of the absolute values is only  $|r| = 0.141$ . Only 6 were significant out of a total of 108.

Again, one should be mindful that the lack of a correlation does not imply lack of endorsement by either group. The positive correlation implies that the no-no cell and the yes-yes cell have “high” endorsement (those who do not endorse a reason also do not endorse a feature



*and* those who endorse a reason also endorse a feature), while a negative correlation implies that no-yes and the yes-no cells have “high” endorsement. The lack of a correlation implies that the percentage endorsement of a feature is the same for both groups of reasons.

Respondents who broadcast to maintain online friends appreciate the privacy of others and the prevention of profiling. Those who use broadcasts to find new friends are less appreciative of privacy of others. Those who use broadcasts to find new follows are more appreciative of secrecy (of content). Those who broadcast for entertainment are less appreciative of personal privacy.

#### *Reasons for Use & Negative Features Associated with the Temporary Nature of the broadcasts*

The associations between the Reasons for Use and the endorsement of the Negative Features of the Temporary Nature of the broadcast are shown in Table 3.52 which also includes the mean percentage endorsement of each feature as a baseline (from Table 3.19). The analysis is similar to the previous.

Table 3.52 Reasons for Use and Negative Features of the Temporary Nature.

	content could be valuable.	cannot know who watched broadcast	reduces number of viewers	need to recreate for each broadcast	enables people to forget me	limits potential popularity of broadcast
Percent Endorsement	52.4	40.5	28.6	21.4	11.9	19.0
Friends Online	-0.229	<b>0.345</b>	0.084	0.127	0.122	<b>0.422</b>
Friends Offline	-0.265	0.093	0.054	0.127	-0.142	0.156
Strangers	-0.072	0.010	0.263	-0.182	0.097	0.017
Find New Friends	0.277	0.004	-0.198	-0.193	0.139	-0.153
Find New Followers	0.000	-0.067	0.083	0.196	0.102	-0.024
Advocate for Chg	0.000	0.074	0.161	0.036	0.136	-0.149
Offer Help	0.062	0.038	0.152	0.242	0.040	-0.044
Provide Advice	-0.132	-0.043	-0.243	0.127	0.066	-0.016
Promote: Profession	-0.265	-0.043	0.203	-0.201	0.275	-0.016
Promote: Business	-0.265	0.093	-0.095	-0.037	0.066	-0.016
Promote: Events	-0.218	-0.173	-0.134	-0.111	-0.078	-0.103
Entertainment	0.158	-0.089	<b>0.339</b>	-0.160	-0.113	-0.149

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ; N = 44 for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

As with the previous, the correlations tend to be small. The average correlation is only  $r = 0.008$  (SD: 0.160, min -0.265, max: 0.422), and the average of the absolute values is only  $|r| = 0.131$ . Only 3 were significant out of a total of 72.

Respondents who broadcast to maintain online friends think that the inability to know who watched and that limits on the potential popularity are negatives. Those who broadcast for entertainment feel that the temporal nature limits the number of viewers.

*Reasons for Use & Information that is Sensitive (to be Kept Private)*

The associations between the Reasons for Use and the endorsement of the Sensitive Information (to be kept private) are shown in Table 3.53, which also includes the mean percentage endorsement of each item as a baseline (from Table 3.23). The analysis is similar to the previous.

Table 3.53 Reasons for Use and Information that is Sensitive (to be Kept Private)

	my face	my voice	my exact GPS location	my approximate location	the visual of my surroundings	the people in my surroundings	my inappropriate behavior	the inappropriate behavior of others
Percent Endorsement	31.0	14.3	66.7	23.8	11.9	26.2	45.2	14.3
Friends Online	0.039	0.188	-0.009	0.294	0.266	0.026	-0.204	0.055
Friends Offline	-0.257	0.035	0.025	0.101	0.066	0.229	-0.079	0.228
Strangers	0.239	-0.142	0.271	-0.023	-0.128	-0.041	-0.168	-0.142
Find New Friends	0.069	0.073	0.052	-0.120	-0.007	0.267	0.208	<b>-0.331</b>
Find New Followers	<b>0.386</b>	0.054	0.251	0.033	0.102	0.236	-0.019	-0.095
Advocate for Chg	-0.032	-0.126	0.239	-0.171	-0.113	0.000	-0.116	-0.126
Offer Help	-0.282	0.008	0.070	-0.088	0.040	-0.108	-0.128	0.008
Provide Advice	-0.112	0.035	-0.250	0.101	<b>0.484</b>	0.076	-0.213	0.228
Promote: Profession	0.033	-0.158	0.025	-0.057	-0.142	-0.076	-0.213	-0.158
Promote: Business	0.178	0.228	0.025	-0.057	0.066	0.076	-0.079	0.035
Promote: Events	-0.141	-0.087	-0.289	-0.118	-0.078	-0.126	-0.190	-0.087
Entertainment	-0.205	0.105	-0.254	0.017	-0.113	-0.183	-0.116	0.105

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ; N = 44 for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The correlations tend to be small. The average correlation is only  $r = -.006$  (SD: 0.162, min - .331, max: 0.484), and the average of the absolute values is only  $|r| = 0.131$ . Only 3 were

significant out of a total of 96.

Respondents who use broadcasts to find New Followers had a higher rate of endorsing the hiding the face. Those who use broadcasts to Provide Advice had a higher rate of hiding surroundings. Those who use broadcasts to Find New Friends endorse hiding the inappropriate behavior of others *less* often.

#### *Reasons for Use & Reasons to Hide Face*

The associations between the Reasons for Use and the endorsement of the Reasons to Hide Face are shown in Table 3.54. The analysis is similar to the previous. Table 3.53 also includes the mean percentage endorsement of each reason as a baseline (from Table 3.25)

Table 3.54 Reasons for Use and Reasons to Hide Face.

	ID	Stalkers	Professional Reasons	Social Reasons	Personal Reasons
Percent Endorsement	45.2	33.3	23.8	23.8	9.5
Friends Online	0.166	0.193	0.075	0.184	0.044
Friends Offline	-0.079	-0.129	-0.057	0.101	0.105
Strangers	-0.023	0.063	-0.194	<b>0.318</b>	0.136
Find New Friends	<b>0.301</b>	0.226	<b>0.321</b>	-0.120	-0.102
Find New Followers	0.187	<b>0.349</b>	0.277	0.155	<b>0.339</b>
Advocate for Change	0.044	-0.216	0.017	-0.171	0.175
Offer Help	-0.254	-0.164	-0.236	-0.088	-0.138
Provide Advice	-0.213	0.013	0.101	0.101	-0.126
Promote: Professional	-0.079	-0.129	-0.057	-0.057	0.105
Promote: Business	0.055	0.013	-0.057	-0.057	0.105
Promote: Events	-0.190	-0.149	-0.118	-0.118	-0.069
Entertainment	-0.116	-0.216	-0.171	-0.171	-0.100

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The correlations tend to be small. The average correlation is only  $r = 0.002$  (SD: 0.165, min  $-0.254$ , max: 0.349), and the average of the absolute values is only  $|r| = 0.141$ . Most are in the small range. Only 4 were significant out of a total of 60.

Respondents who use broadcasts to maintain contact with strangers had a higher rate of endorsing the hiding of the face for social reasons. Those who use broadcasts to Find New Friends endorse high higher rates of endorsing the hiding of the face for ID theft and for professional reasons. Those who used broadcasts to Find New Followers had a higher rate of endorsing the hiding of the face for fear of stalkers.

*Reasons for Use & Reasons to Hide Voice*

The associations between the Reasons for Use and the endorsement of the Reasons to Hide Voice are shown in Table 3.55. The analysis is similar to the previous. Table 3.55 also includes the mean percentage endorsement of each reason as a baseline (from Table 3.25)

Table 3.55 Reasons for Use and Reasons to Hide Voice.

	ID	Stalkers	Professional Reasons	Social Reasons	Personal Reasons
Percent Endorsement	26.2	16.7	14.3	14.3	14.3
Friends Online	0.238	0.248	0.188	0.055	0.188
Friends Offline	0.076	0.008	0.035	0.035	0.035
Strangers	-0.041	-0.156	-0.142	-0.142	0.066
Find New Friends	-0.160	0.017	0.073	0.208	-0.061
Find New Followers	-0.118	0.013	-0.095	-0.095	<b>0.351</b>
Advocate for Change	-0.183	0.079	0.105	-0.126	0.105
Offer Help	-0.251	-0.189	-0.173	0.008	-0.173
Provide Advice	-0.076	0.008	0.035	0.035	0.228
Promote: Professional	-0.076	0.008	0.035	-0.158	0.035
Promote: Business	-0.076	0.189	0.035	-0.158	0.035
Promote: Events	-0.126	-0.095	-0.087	-0.087	-0.087
Entertainment	0.000	-0.138	-0.126	-0.126	-0.126

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ; N = 44 for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The correlations were small with an average of  $r = -0.015$  (SD: 0.131, min -0.251, max: 0.351), and the average of the absolute values is only  $|r| = 0.107$ . Only 1 was significant out of a total of 60.

Respondents who broadcasts to Find New Followers had a higher rate of endorsing the hiding of the voice for personal reasons.

*Reasons for Use & Reasons to Hide Location*

The associations between the Reasons for Use and the endorsement of the Reasons to Hide Location are shown in Table 3.56. The analysis is similar to the previous. Table 3.56 also includes the mean percentage endorsement of each reason as a baseline (from Table 3.27)

Table 3.56 Reasons for Use and Reasons to Hide Location.

	Stalkers	Others I do Not Want to See	Government Monitoring	Professional Reasons	Social Reasons	Personal Reasons
Percent Endorsement	69.0	50.0	7.1	14.3	23.8	14.3
Friends Online	0.046	0.177	0.128	0.322	0.075	0.055
Friends Offline	-0.133	0.018	<b>0.418</b>	0.035	-0.057	0.035
Strangers	0.106	0.088	-0.097	-0.142	-0.194	-0.142
Find New Friends	0.013	-0.147	-0.042	-0.061	0.321	-0.061
Find New Followers	0.117	0.130	0.037	-0.095	0.155	<b>0.351</b>
Advocate for Change	0.061	<b>0.331</b>	-0.086	0.105	0.017	<b>0.335</b>
Offer Help	-0.080	-0.042	0.129	-0.173	-0.088	0.008
Provide Advice	-0.133	0.151	-0.107	0.035	-0.057	0.035
Promote: Professional	-0.133	-0.115	-0.107	0.035	-0.057	-0.158
Promote: Business	-0.133	0.151	-0.107	0.035	0.101	-0.158
Promote: Events	<b>-0.303</b>	-0.209	-0.059	-0.087	-0.118	-0.087
Entertainment	0.061	0.014	-0.086	-0.126	-0.171	-0.126

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ; N = 44 for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The correlations tend to be small. The average correlation is only  $r = -.001$  (SD: 0.148, min  $-0.303$ , max: 0.418), and the average of the absolute values is only  $|r| = 0.120$ . Five of the 72 were significant.

Respondents who use broadcasts to maintain contact with Friends Offline advocated hiding location for Professional Reasons. Those who broadcast to Find New Followers advocated for hiding location for Personal Reasons, as those who broadcast to Advocate for Change. Those who broadcast to Promote Events advocated for the hiding of location to thwart stalkers.

*Mood and Reasons to Hide Face*

Mood while broadcasting was collected (overall categories) in 4 categories (Happy, Sad, Angry, Worried) but the categories of Compelled (because it implies mood is irrelevant), Stimulants (because it is mood-altering) and Driving (because of the special implications for broadcasting and mood). These were collected using a five-point scale. The associations between Mood (while broadcasting) the reasons to hide one’s face are shown in Table 3.57

Table 3.57 Mood and Reasons to Hide Face.

	ID	Stalkers	Professional Reasons	Social Reasons	Personal Reasons
Happy	-0.105	-0.094	0.067	0.067	0.280
Sad	0.095	0.159	0.201	0.003	0.059
Angry	0.124	0.225	0.252	-0.151	0.247
Worried	0.291	0.229	0.228	0.173	0.116
Compelled	0.144	0.226	0.194	0.158	0.081
Stimulants	0.087	0.098	<b>0.420</b>	-0.124	0.181
Driving	0.019	0.092	0.234	<b>0.364</b>	-0.192

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ; N = 44 for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).



The correlations tend to be small. The average correlation is  $r = 0.127$  (SD: 0.142, min  $-0.192$ , max: 0.420), and the average of the absolute values is only  $|r| = 0.141$ . Two were significant out of a total of 42.

Those who broadcast while under the influence of stimulants tended to endorse the hiding of faces for professional reasons more often, and those who broadcast while driving tended to endorse the hiding of the face for social reasons more often.

### *Periscope Users*

Those respondents who used Periscope were given the opportunity to provide more information about their use. This tended to revolve around the location feature of Periscope. A total of 33 participants completed this section (though some items had missing data).

#### *Locations and Knowledge of the Location Features*

Knowledge of the location features of Periscope was probed with two questions. The first asked if they knew of the location feature. The second asked if they knew of the setting for the location feature. There were only 23 responses. Missing values were not assumed to be zero (lack of knowledge), though that might likely be a valid approach. The associations of knowledge about the location feature with the location of the broadcast are presented in Table 3.58.

Table 3.58 Periscope Users: Knowledge of Location Feature and the Location of Broadcasts

	Work	Home	Public	Parties	Driving
Knows of Location Feature	<b>-0.462</b>	-0.109	-0.058	-0.128	-0.278
Knows of Location Setting	<b>-0.521</b>	-0.064	-0.190	-0.224	-0.313

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 23$  for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The average correlation is  $r = -0.235$  (SD: 0.160, min  $-0.521$ , max:  $-0.058$ ), and the average of the absolute values is only  $|r| = 0.235$ . Note that only two are significant because the sample size is substantially reduced.

The interesting observation is that all are negative. This implies that people with knowledge of the location attribute of Periscope broadcast *less everywhere*, which begs the question of “where do they broadcast”. In fact, the negative correlations are caused by a bit of an artifact: most respondents do *not* know of the location attributes (e.g., 18 of 23 for the knowledge question). Thus, one cell of the 2x2 design has most of the data, and this causes the correlation. Table 3.59 makes the results clearer.

Table 3.59 Periscope Users: Knowledge of Location Feature and the Location of Broadcasts

		<i>N</i>	Work	Home	Public	Parties	Driving
Knows of Location Feature	no	18	55.6	88.9	66.7	55.6	27.8
	yes	5	0.0	80.0	60.0	40.0	0.0
Knows of Location Setting	no	17	58.8	88.2	70.6	58.8	29.4
	yes	6	0.0	83.3	50.0	33.3	0.0

In Table 3.59, 18 of 23 respondents do not know of the location feature (Column N). Of that 18, 55.6% broadcast at Work, 88.9% broadcast at home, et cetera. However, 5 of 23 respondents do know of the location feature (Column N), and of that 5, 0.0% broadcast at work, 80.0% broadcast at home, et cetera. The lack of significance in the correlations is due to the fact that the percentage for the yes and no groups are about the same. The only significant result is for the broadcast at work, where the percentages are dramatically different.

The general synopsis is that knowledge of the location features of Periscope does not seem to affect the location of broadcast, except for broadcasts from work.

#### *Locations and The Duration of the Saved Video*

The duration of the saved video was probed with four items: The first asked how often the broadcast was saved for 24hour (using a five-point scale from "never" (0) to "always" (4)). The second asked how often broadcasts were saved for less than 24 hour using the same scale. The third asked how often broadcasts were deleted immediately using the same scale. The fourth asked how often the broadcasts were saved for “some other value” using the same scale. The

data from the fourth replicated the first, so it is not analyzed further. Location is a dichotomy (binary) so the analysis of correlations is equivalent to that of a t-test, in which each location is a grouping factor (See Table 3.60).

Table 3.60 Periscope Users: Location and Retention Intervals

	Work	Home	Public	Parties	Driving
Available 24hour	0.149	-0.062	-0.015	-0.105	<b><i>-0.594</i></b>
Available <24hour	-0.011	-0.030	0.120	<b><i>0.592</i></b>	0.060
Delete Immediately	<b><i>-0.372</i></b>	<b><i>0.358</i></b>	-0.059	-0.160	0.006

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ; N = 23 for all comparisons.

These are equivalent to phi-correlations ( $\Phi$ ).

The average correlation is  $r = 0.043$  (SD: 0.198, min -0.316, max: -0.530), and the average of the absolute values is  $|r| = 0.160$ . These are small, but 4 of 10 are significant. The correlations imply that those who broadcast at work are *less* likely to delete immediately, while those who broadcast at home are *more* likely to delete immediately. Those who broadcast at parties are more likely to retain the broadcast for some period less than 24 hour, while those who broadcast while driving are more likely to retain the broadcast for the full 24 hour. These findings do have some post-hoc reasonableness.

#### *Audience and Reasons to Keep broadcast*

Because Periscope users can save a broadcast, they were asked why they would save it. This was then compared with the level of privacy because a saved public broadcast is more of a concern than a saved private broadcast. Table 3.61 presents the analysis of each reason.

Table 3.61 Periscope Users: Audience and Reasons to Keep Video

	Private	Public	Both	<i>F</i>	<i>p(F)</i>	$\eta^2$
	9	7	12			
Useful	88.9	33.3	85.7	3.933	0.018	0.407
Review	55.6	50.0	42.9	0.126	0.944	0.013
Requested	22.2	8.3	14.3	2.104	0.121	0.218
Re-evaluation	22.2	25.0	57.1	2.385	0.090	0.247
Self-Evaluation	44.4	50.0	42.9	0.632	0.600	0.065
knowledge of Viewers	33.3	58.3	28.6	0.816	0.496	0.084
Block Viewers	22.2	16.7	14.3	0.059	0.981	0.006
Follow Viewers	22.2	41.7	28.6	0.388	0.763	0.040
Get Feedback	44.4	66.7	28.6	0.932	0.438	0.096

There is a significantly higher tendency to retain a private video because it is useful. The other reasons did not differ as a function of the level of privacy (though some might say that re-evaluation was “marginal”). Note that the effect sizes for Useful, Requested and Re-evaluation are “respectable” ( $\eta^2$  should be interpreted like  $r^2$ ), so one implication is that a larger sample size might show more effects for these attributions (See Table 3.61).

*Audience and Reasons to Delete broadcast*

In a similar manner, because Periscope users can choose to delete a broadcast immediately, they were asked why they would do so. This was then compared with the level of privacy because a saved public broadcast is more of a concern than a saved private broadcast (See Table 3.62).

Table 3.62 Periscope Users: Percent Endorsement for Audience and Reasons to Delete Video

	Private	Public	Both	<i>F</i>	<i>p(F)</i>	$\eta^2$
	9	7	12			
embarrassing	22.2	25.0	42.9	0.947	0.431	0.098
rude	33.3	50.0	28.6	0.547	0.654	0.057
sexual	11.1	41.7	0.0	2.974	0.048	0.308
gossip	22.2	50.0	14.3	1.053	0.384	0.109
religious	0.0	41.7	0.0	4.565	0.010	0.472
political	11.1	33.3	14.3	1.606	0.209	0.166
protect privacy: me	55.6	75.0	85.7	1.190	0.331	0.123
protect privacy: others	44.4	58.3	28.6	0.909	0.449	0.094
avoid misappropriation	22.2	41.7	28.6	0.317	0.813	0.033

There is a slightly higher tendency to delete a video that contains inappropriate sexual or religious comments, when it is Public. Oddly, despite the international character of the sample, inappropriate political comments were not singled out, and in fact, were low across the board.

### 3.3 Discussion

#### 3.3.1 Participants Demographic

Users of temporal live video streaming apps (Live Video Broadcasting apps, LVB) come from a variety of backgrounds. In the current study, users were about 57% female having the full range of age and educational backgrounds. Despite the use of streaming video apps, their self-reported comfort with technology ranged from “very uncomfortable” to “very comfortable” and their self-reported knowledge of security ranged from “no knowledge” to “expert”. Although the mean for comfort was toward the higher more comfortable end of the scale, the mean for knowledge of security was “minimal”. Hence, a large number of people are using apps without any genuine knowledge of security: A few are using them without comfort and security.

### 3.3.2 Live Video Apps Use

The actual apps used seemed to favor Periscope over the others. Why this would happen is not clear. The demographics did not differ between apps (e.g., sex, age, education, comfort with technology, knowledge of security) and the pattern of use did not differ between apps (e.g., reasons for use, broadcast categories, audience, or planning). As such, it cannot be one of these attributes though it may be some other feature such as "ease of use" or a private broadcast feature. It is also possible that Periscope simply has more exposure because it is owned by Twitter. Nonetheless, the positive aspect of this is that researchers need not worry about the particular app when exploring other issues related to live video broadcasting.

The most significant reason for use is to maintain contact with friends (online or offline) or online strangers. However, some use apps to promote their work or profession, or to find new friends, and offer advice and help. This shows the difference of usage between live video broadcasting apps in which the broadcaster can be seen but the viewers cannot, and video chat apps (e.g., Facetime) where users can see each other while chatting. Video chat apps are mainly used for maintaining strong relationships (e.g., friends, family; Judge & Neustaedter, 2010; Massimi & Neustaedter, 2014; Wang, Mughal & Juhlin, 2015).

Oddly, those who use LVB apps to maintain contact with old family and friends do *not* use these apps to find new friends (and vice versa). This may be a consequence of the fact that 28 of 44 respondents use Periscope (16 of 44 exclusively). This is the only app that allows private broadcasts, and as such, the sample may be weighted to those who predominately use such apps to maintain private (existing) relationships.

This work also shows that live video broadcasting is used in a self-promotion manner like YouTube or similar videos — to seek popularity or demonstrate skills (Courtois et al., 2013). There are numerous YouTube videos that promote businesses. However, although live video broadcasts may be used for professional or business promotion, the mode of operation must be different because the video is temporary. The temporal nature would be most useful when promoting special events (or sales events) where a permanent record is not desired or useful. When used in this manner (e.g., profile or business promotion; advocacy and helping), live video broadcasting might have promotional benefit because the immediacy and spontaneity (and visual identity) that they offer provides a way of increasing trust in viewers/customers/clients.

### **3.3.3 Categories of Broadcasts and Privacy**

For the category of broadcast, there is a good mix of Formal and Informal broadcasts and a good mix of Self and Other broadcasts, and most respondents (75%) used a variety of categories. The audience was evenly split between exclusively private, exclusively public and both, but an important implication is that 53% of the respondents are engaged in public broadcasts at some point (a further 16% could not be categorized, so this figure may be higher). Only Periscope offers a private video feature. The fact that more than half of broadcasts are public could be one reason why such apps do not offer a privacy setting. On the other hand, almost half are private so all apps should offer it. It is also possible that participants do not care about the privacy of the broadcast.

With respect to planning or spontaneity, 73% of respondents indicated the use of spontaneous broadcasts. Only 14% used exclusively planned broadcasts (a further 9% did not provide data). Planned broadcasts tend to be associated with Formal broadcast (particular Formal broadcast of Self). Spontaneity means Broadcasters do not plan or prepare for the live video broadcast. This can help to ensure the likeability (a tendency to recommend a person or product to others in a positive way) the broadcast (e.g., self-disclosure can enhance intimacy), but privacy issues are more likely to arise because of that same self-disclosure. This form of broadcasting is different from the case of YouTube videos where the lack of a live component at least encourages some review and editing prior to posting (Misoch, 2015). One would expect people to be more mindful or concerned about their reputations when planning

### **3.3.4 Broadcast Locations and Privacy Issues**

The most common location for broadcasts was at home (79%) followed by public places (70%). All other locations, including while driving, were endorsed by less than 50% of the respondents. There was a general trend for broadcasts of Self to be at home and broadcasts of Other to be in public. Broadcasts at work were predominately formal, while broadcasts at parties were predominately informal. The survey does not address why people broadcast in various locations. Most choices are likely dictated by the location of the desired content. However, some choices may be matters of convenience (e.g., home), comfort (e.g., home) or security (e.g., work). The

home is also a more fitting place for candid self-expression particularly if the broadcast is private. Work and home likely offer the availability of a stable and relatively less expensive Internet (or Wi-Fi) connections because video broadcasts can consume a substantial amount of bandwidth. The locations have different issues for security and privacy. Broadcasting at home can reveal many details about the broadcaster's identity, location (especially for the apps that have access to the broadcaster's location), and home environment, which can lead to problems like ID theft, simple property theft or vandalism, or even social ridicule. On the other hand, broadcasts in public (including parties or while driving) may capture the images and actions of other people without consent. There is also the possibility that strangers may see or hear things that were intended to be private. Both of these are particular concerns when combined with spontaneous, public, broadcasts. broadcast at work would seem to have fewer issues of privacy (e.g., other employees know of the broadcast) and security (e.g., most work places have some form of security), but that option is only available if sanctioned by employers.

### **3.3.5 Mood and Privacy**

With respect to mood, the results show that people mostly broadcast when they are happy (88%), worried (33%) or required to do so (e.g., work: 49%). Since live video broadcasts are used for usefulness and enjoyment, it would be predicted that the mood would be, in general, happy. Happiness is also correlated with extroversion, emotional stability, and openness to new experience, the three personality traits of frequent social media users (Correa, Hinsley & De Zuniga, 2010). Interestingly, only a few reported that they broadcast under the influence of stimulants. This is consistent with the low endorsement of parties. It is also possible that this value is an underestimation because people may decline to disclose sensitive information on surveys (Acquisti et al., 2015). Even still, the reported 7% could actually turn into a large absolute number if the number LVB app uses continues to increase (e.g., if 1,000,000 people use these apps, 70,000 do so under the influence of stimulants). Because stimulants can impair judgment, there are more issues across the board for privacy (self and other) and security.

Most broadcasters (62%) are not limited in their amount of use. For those that are, there are a mix of expected reasons: time, costs and fears about security. Fears about security were not a dominant issue. This may imply a lack of understanding about issues for privacy and security.



### **3.3.6 Privacy Concerns with Broadcasts**

Concerns about lawsuits and employers are lower than the rest. This may be a failure to consider the issue, or because broadcasters genuinely believe that employers will not see their broadcasts or that lawsuits are not possible because broadcasters do not (generally) use their proper names. However, as the issues with employer views of Facebook accounts have shown, this may be a false sense of security. In addition, as facial search algorithms improve, it will be easier for employers (or other security firms) to search for and find particular broadcasters. In addition, it will become easier to search for particular individuals who may have been captured in such videos, or even particular locations. That is, what happens now is just the beginning, and it is important for users — and developers — to consider privacy and security now. Public broadcasts may be viewable to the world: No one can accurately predict who will do what with the information.

### **3.3.7 Knowledge about Temporal Live Video Broadcasting Apps**

Overall, 78% of respondents know that live video apps do not enable the viewers to save the broadcast: That 78% includes 35% who know that Periscope has the capability to save broadcasts for up to 24 hours. Similarly, 73% of respondents know that the apps do not allow viewers to replay the broadcasts: This 73% includes the 30% who know about the special abilities of Periscope. Generally, respondents have good knowledge about the temporal nature of the broadcasts, but oddly, about 35% do not have this knowledge. Note that those who know about the inability to save broadcasts also know about the inability to replay broadcasts. It may be the some broadcasters do not care. It may be that they are new to the live broadcasting.

The level of concern shown for Social Reputation, Physical Harm and Economic Harm are more reasonable (2 out of 3) but the statistics imply that some people are simply not concerned (the minimum level is 0). Recall that slightly more than half of all broadcasters engaged in public broadcasts. These individuals need to be particularly concerned about privacy. It is possible that concerns for Social Reputation are higher because LVB apps represent the next wave of social media. These “early adopters” may be the individuals who are more highly motivated by social concerns. Physical harm is likely in the forefront because it is presented

everywhere in the mass media (e.g., television, news reporting) so individuals are hyper-vigilant.

### 3.3.8 Pros and Cons of Temporary Nature Live Broadcasts

The temporary nature of the broadcast was likely a design feature implemented because of the enormous storage requirements that would be demand if “every” broadcaster wanted permanent storage for every broadcast ever created. However, it is also a positive feature for privacy and security.

Most respondents endorsed the idea that the temporary nature protects one's privacy. However, this does not imply that people use temporal live video apps because they believe it serves their privacy. They likely use them because they want to have a convenient way to make and send a video. The alternatives are more work (e.g., create, then package and then send the video). However, some participants are aware of the privacy and security benefits. For example, 33% believe that the temporary nature limits unwanted viewers, 29% believe it limits the ability of people to create profiles of the broadcaster, 26% believe it protects the contents, and 24% believe it protects the privacy of others. Generally, there seemed to be two groups: one that endorses privacy protection, and another that endorses all other positive features. Nonetheless, these percentages are not high. One-third of respondents did *not* endorse privacy protection, and more than two-thirds of respondents did *not* endorse the rest of the reasons.

Previously noted that the number of positive features endorsed was *positively correlated* with the number of negative features. That is, people see both positive and negative features; it is not that some see only positive features while others see only negative features (that would imply a negative correlation). Therefore, it is likely that most respondents do not endorse the positive features of the temporary nature of broadcasts because the temporary nature has negative aspects as well. More than half (52%) disliked the temporary nature because the content could be valuable. This is related to the need to recreate it each time. Furthermore 41% complained that one could not know who had watched a video. Many respondents understood that the temporal nature had both pros and cons, (i.e., some broadcasters see more pros and more cons). There is some question about how this will evolve over time. The desire for privacy might win out over the value of the content. What will likely happen is that more apps will offer temporary storage and more broadcasters will accept that.

### **3.3.9 The Desire for Privacy on Live Video Broadcasts**

There are particularly strong correlations between the desire to identify viewers, to identify followers, and to block viewers who take screenshots. Those who want to know about viewers who access GPS location are a distinct group. The desired feedback was a clear sign of privacy and security concerns. Most respondents (81%) want to know who viewed their location (particularly those who viewed GPS data) — almost half (50%) want the ability to identify viewers, identify followers and to block viewers who take screenshots of the broadcasts. This may imply that there are viewers who are unfriendly and commit negative comments or may be constitute threat to the broadcaster, which assure there is a need to increase the level of privacy to the broadcaster. In the future, apps will need to provide these features in a broadcasters/viewer balanced fashion (e.g., viewers may choose the reveal their identity, and broadcasters may be given the chance to block anonymous viewers). This meshes with the increased ability to have private audiences (currently a Periscope function). On the other hand, service providers may not “like” privacy because it implies the use of resources (e.g., bandwidth, temporary storage) with any associated revenue stream (e.g., advertising, exposure). A new model based on a subscription service may emerge from all of this.

### **3.3.10 The Privacy of Sensitive Information**

Issue of privacy and security also manifest in the attributes that broadcasters want to hide. Previously noted that there are only 3 not strong significant correlations; hiding face with hiding GPS; hiding general location with hiding surrounding visuals; hiding my inappropriate behavior with hiding inappropriate behavior of others). This implies that every respondent has “idiosyncratic combinations” of desires. That implies that companies must supply all as “optional features”. Consistent with the previous, about 67% of broadcaster want the ability to hide their location (GPS). It is the exact location that matters. Only 24% want the ability to hide their approximate location. Other features were endorsed much less often: hiding face (31%), hiding voice (14%), hiding other people (26%). Interestingly, 45% would like the app to hide their “inappropriate behavior” but how that would be accomplished is an unknown. What is “inappropriate”? It likely varies across individuals and situations. How a program could be

trained to recognize that in a context sensitive manner (e.g., “screaming” might be appropriate for a party broadcast, but not for a formal work broadcast). For this reason, in our follow-up study, we design a generic mechanism to protect visual privacy of the broadcaster. Nonetheless, the results imply that developers will need to provide more features. The most cited reason for hiding location, face and voice were ID theft and stalkers (or other unwanted people). Broadcasters were not particularly concerned about government or employer monitoring.

### **3.3.11 Periscope Users and Privacy**

#### *Type of Broadcasts Audience*

Results show that “friends offline” and “family” are the most common audience for the participants. In this case, the ability to make private broadcasts using Periscope turns Periscope into a video chat app like Facetime in sense of that is about socializing with known people. The channel characteristics are different (i.e., Periscope is uni-directional), but such differences have a use (e.g., when the broadcaster and viewer live in very different time zones).

#### *Knowledge about Periscope*

Generally, Periscope users are aware of the fact that their broadcast can be saved for up to 24 hours. However, about two-thirds of respondents reported that they delete some broadcasts immediately because they want to protect their privacy. Thus they are aware of privacy issues. However, the same percentage indicated that they keep some broadcasts because they are useful. Note that very few respondents reported that the “always” keep for 24 hour or delete immediately. This implies that most broadcasters are selective about the time frame for saving.

#### *Categories of Periscope Broadcasts*

It seems that these broadcasts are formal, and maybe they are planned. This confirmed the negative aspects of temporary nature endorsed by respondents in earlier questions. This is dominant where people use the live video broadcasting as promotion to their products (business), or when they advocate for important issues, or try to help people. From this perspective, we can see that live video apps could be considered as task-oriented system, especially that broadcasts have high possibility to be viewed publicly to the world.

### *Periscope's Critical Feature*

Periscope reveals location by default. However, 46% of respondents indicated that they reveal their location “generally” and 27% reveal it while driving. When we asked about the benefits of revealing one’s location, the endorsements of any reason were not high. The highest was only 42% for “emergencies”. At the other end of scale, almost no one endorsed revealing location for “the comfort of remote awareness”. On the other hand, fully 70% would specifically hide their location to avoid providing the location of their home and 76% to avoid being found by people. Generally, Periscope users cited more negative than positive reasons.

## **3.4 Limitations and Future Work**

The current survey has provided a wealth of information about the use of temporary live video broadcasting apps. However, as with any research, there are limitations to the generalizations that can be made on the basis of this data. Limitations almost automatically lead to future work, so the limitations and other insights lead to several recommendations for continuing this line of investigation.

Firstly, it is acknowledged that the selected research design is an anonymous survey. Survey designs have many advantages and disadvantages. They rely on self-report, which is not verified. However, the current survey is a “fact-finding”, low-risk form of data collection. None of the collected data is of a controversial nature (i.e., we did not ask about sensitive personal, cultural or political, topics, we did not ask about illegal or immoral behaviours). Hence participants would not be inclined to misrepresentation or exaggeration. Self-reports rely on memory, and human memory is fallible, but in this case, the survey is asking about “current” behaviour, so issues for memory are minimal. The only concern for the current questionnaire is the items that tap the use of stimulants. We have acknowledged that there may be some (systematic) under reporting on this item. It should be noted that we did not ask about any of the illegal aspects of drug use (e.g., what drugs, when were drugs used, where were drugs obtained from), and we did not ask about any associated illegal activities (e.g., driving while intoxicated). We are concerned about stimulants for their impact on broadcasting, but we tried to make the

items about stimulant use as unobtrusive as possible.

This survey (as most) is voluntary. There may be a self-selection bias. However, it is likely that every existing survey suffers from the same problem, except those that are legally binding (e.g., government mandates surveys like the census, or the Labour Force Survey of Canada). There is no solution to this problem. In addition, the survey used “yes/no checklist” items, and the default value was zero. If the response was zero, we cannot know if the respondent read and responded to the item, or skipped the item.

### **3.4.1 Validity**

Because this is an anonymous survey that relies on unverified self-report, there is some concern about validity. Validity is usually assessed by comparing the current tool with other (hopefully verified) tools. However, there are no other tools so that is not possible. Alternatively, one can compare the current survey to other tools (e.g., other surveys) that have some degree of conceptual overlap. However, that type of work is an entire research program, which would have detracted from the main goal. In addition, the goal here is not questionnaire development. The goal was to collect some basic facts about app use. As noted above, there is no reason to suspect systematic bias on the part of all respondents (random errors are expected).

### **3.4.2 Reliability**

Because this is an anonymous survey that relies on unverified self-report, there is also some concern about reliability. To assess reliability, the classic approach is to give the same questionnaire twice to the same people. The consistency of responses is “test-retest” reliability (Swerdlik and Cohen, 1999; Shultz and Whitney, 2005). Test-retest reliability is not an option with anonymous surveys. An alternative is to provide two (or more) slightly different versions of the same question within the one questionnaire. This is often called internal consistency. It can be seen that it is, in fact, a miniature form of test-retest reliability (the second version is a re-test of the first). That is the standard approach in questionnaire design. Multiple versions of the same question also allow one to tap the breadth of a concept (i.e., different people may see the same concept in slightly different ways). Parts of the current questionnaire did this.

For example, there were two assessments of mood while broadcasting and both assessments provided the same results. The results of the Periscope section supported the main section. Questions about concerns showed a similar pattern to questions about the information that should be considered sensitive (keep private) and to questions about desired feedback. For example, not knowing who viewed the broadcaster's location was the highest concern, considered the most sensitive, and was the most requested type of feedback. The third highest concern was for social harm, which was related to the second highest item of sensitive information ("my inappropriate behavior"). Internal consistency can also be checked by an examination of the logical relationships between questions. Those relationships should "make sense" — this was discussed in the current results as the "pattern" of results (particularly the pattern of correlations). For example, within moods, respondents were asked about happy and sad. Logically, there should be a relationship in that those who broadcast more often when happy should broadcast less often when sad. In this case, there was no relationship (the correlation was zero), but that was a consequence of the way the questions were worded. As noted above, much of the questionnaire is about collecting facts.

The second major limitation is the sample: It is small, and focused on North America and the Middle East. Generalizations beyond that group should not be made. In addition, a large proportion of respondents who started the survey did not complete the survey (only 44 of 75). This is cause for concern because it may imply that only a particular demographic was sufficiently motivated to complete the survey. It also implies that the survey "needs work", in the sense that it may be too long or too onerous.

The issue of a small and localized sample is related to the problem of recruitment. Survey methodology has a long history and there are many recommendations for achieving a high and appropriate response rate. However, these recommendations apply to "standard" postal, telephone or e-mail surveys (e.g., (Sheehan, 2001)). Currently there is a general lack of information about how to achieve high response rates from the appropriate population when using online surveys in general, but also more so with online international anonymous surveys. That is, despite an extensive search, we could not find any articles specifically documenting means of ensuring response rates to general online surveys with an unspecified audience (i.e., respondents with *no* other means of access such as email). For example, Archer (2008) did not include any recommendations about recruitment in his article entitled "Response Rates to Expect from Web-Based Surveys and What to Do

About It". Archer (2007) provided recommendations but they all revolve around knowledge of the email addresses of potential respondents. Furthermore, even with a targeted audience (known email and postal addresses), Kongsved, Basnov, Holm-Christensen & Hjollund (2007) noted that response rates for the Internet surveys were low when compare to a directly equivalent paper and pencil version. While such questions are not specific to the current work, their impact on the current work is notable. For example, live video broadcasting apps are relatively new. As such, there are no webpages specifically created for these apps. Recruitment relied on hashtags through social media (Twitter, Facebook) and these were only partially successful.

For future work, it would be nice to obtain a broader sampling from the international community. The current sample under-represented Europe, Asia and Africa. On a similar note, it is advised that the current survey be translated into other languages before it is refined. The use of English is worldwide and it is still the dominant language of the web (at least, outside China). As such, a few more iterations with English would likely help.

A third major limitation is that the survey does not (generally) collect data about "why". That is, the survey is fact-based. For example, there is considerable data about the locations of the broadcast, but no data about the "why" certain locations are chosen. The fact is that most people broadcast from home, but we do not know why that is the case. We did speculate about why, but those remain as reasonable speculations. Another example is the bigger question of why people choose to use live video broadcasting apps at all. We did collect data on the Reasons for Use (e.g., to maintain contact with family or friends) but these reasons do not explain why live video broadcasts were chosen over other apps such as Skype, Facetime or even YouTube. That is, maintaining contact with family and friends was an important Reason for Use. Yet, Skype and Facetime would be far better apps for that purpose (they allow a dialogue). Why use live video broadcasting apps? The same is true for business or self-promotions. The only area where live video broadcasting apps have a clear advantage is in the spontaneous transmission of current events. As with locations, we can speculate.

As such, future work should be directed as understanding the Reasons for Use. This would likely require an interview approach to uncover the most likely explanations, which could then be converted to a questionnaire format to collect data from a wider sample. Similarly, future work should be directed as the reasons behind the various privacy and security concerns. For example, why are people concerned about physical harm? It seems to be an unlikely response to



a public broadcast that is international in scope. That is, the broadcaster would need to create a great deal of animosity to cause a viewer to travel to a great distance just to cause physical harm. Similarly, what type of social harm do broadcasters think a broadcast can cause. Most broadcasters do not seem to remember the lessons of Facebook and employer monitoring (e.g., people losing jobs over Facebook posts, implications that people were not hired because of Facebook posts). Government monitoring (particular in the USA with the Patriot act) is also not the issue it might need to be. More generally, the specific details about the concerns or risks need to be explored.

More generally, it must be remembered that all inferences are tied to the questions asked. The data collected herein is descriptive (facts). As such, inferences about why people engage in particular behaviors (why they answered they way that they did) are speculative. We can (and did) speculate, but those speculations must be treated with caution until verified in future work.

For future work, the current survey can be refined in many ways. For example, the Reasons for Use should be expanded to include “entertainment”. The Reasons for Use could be reduced in other ways (e.g., altruism was not selected often). The current survey likely collects too much data about the apps that were used. The pattern of use did not differ across apps, so less detail could be collected. The level of detail about the Categories of Use (i.e., Formal BC of Self, Informal BC of Self, Formal BC of Others, Informal BC of Other, Non-Human BCs) could be reduced (because most respondents used multiple categories). That is, space in the questionnaire could be reallocated to the collection of more data about privacy and/or planning and/or location and/or mood. That is, instead of designing questions (items) that cross Category of Use with each of privacy, planning, location, and mood, design questions (items) that cross privacy with planning, and/or planning with location and/or planning with mood.

For future work, the Concerns that broadcasters have need to more specifically tied to the ways in which broadcaster think those concerns should be dealt with. Sensitive Information (to be Kept Private) needs to be tied to specific Concerns. For example, one concern is ID theft. How would that specific problem be prevented? Do people believe the blurring the face would prevent ID theft? A more general question is “Does face blurring prevent ID theft?” Generally, more research is needed on how these apps can alleviate these concerns (see Study 2 of the current work). In addition, when broadcasting while driving we do not know how this was done.

More investigation is needed about how and why these broadcasts created, and whether these broadcast require attention.

Finally, for consideration of future work, the current survey provides useful insights into the type of “background” questions that other research should consider when designing research questions into other aspects of live video broadcasting. For example, focusing on which apps are used may be a waste of resources, but a simplified set of Reasons for Use is essential because there seems to be subgroups (e.g., those who use such apps for maintaining relationship, for finding new relationships, for promoting business or professions). The level of privacy can be simplified. The degree of planning may need to be expanded. Moreover, further investigation is needed into the use of stimulant while broadcasting. The current research did gather some preliminary data but did not delve into the topic. However, gathering this type of data may be more difficult. Firstly people are often reluctant to present information that casts themselves in a negative light (the self-serving bias). Secondly, some stimulant commonly used may be illegal in the home country of the broadcaster. As such, they may be reluctant to reveal such information even in an anonymous survey. Thirdly, given the nature of some stimulants, they may not remember the details of such broadcasts (e.g., the audience, their location(s), other aspects of mood).

## **CHAPTER 4 DESIGN OF PRIVACY AWARENESS MECHANISMS**

To address some of the privacy issues that have been discussed, we designed three dynamic real-time awareness prototypes called *Location Viewers Feedback prototypes (LVFPs)* to provide feedback to the live video broadcaster; specifically, this mechanism is intended to notify the broadcaster that his/her location is currently being disclosed to the public. Addressing similar concerns, we also designed three *visual privacy awareness prototypes (VPAPs)* that protect privacy by obscuring identity. These two interventions are presented and described in the sections that follow. It is important to note that not all broadcast viewers view a broadcaster's location, but location viewers are those who are already viewing the broadcast. In this chapter, after describing the methodology of designing *LVFPs and VPAPs*, we describe how we conducted the experiment to evaluate the prototypes. Then, we present the results of the two experiments based on participants' feedback. We then compare and discuss our prototypes designs, highlighting the suggestions for improvement and design implications of *LVFPs and VPAPs*. Finally, we highlight the limitations and future work of *LVFPs and VPAPs*.

### **4.1 Location Viewers Feedback Prototypes (LVFPs)**

#### **4.1.1 Theoretical Foundation:**

Privacy nudge or soft paternalism in the case of insecure communication takes the form of alerts to inform the user about potential risks when information is disclosed (Balebako et al., 2011).

We propose three different prototypes for location viewers based on the concept of privacy nudge or called soft paternalism to notify the live video broadcaster about the viewers who are viewing his/her location. These prototypes differ primarily with respect to the manner in which they provide information to the broadcaster. LVFPs might be implemented as a part of a larger

privacy management system, intended to be dynamic and real-time, showing moment-to-moment of viewers' movements (who are looking at the location) around the broadcaster's location. Not only that, but it also provides information about the location viewers (e.g., username, distance from broadcaster location). The "Vagueness" technique is used to inform the broadcaster about the location of viewers. This technique describes the distance in terms of how far or close a viewer is from the broadcaster's location. The prototypes also show whether those viewers are getting closer or further away from the broadcaster's location.

The particular functions of these prototypes were suggested by our survey results, which indicated that participants want to know detailed information about those who viewed the location. Those results showed that, on a more basic level, many Periscope broadcasters were not even aware that their location is visible to the public.

Our overall goal for designing *Location Viewers Feedback (LVF)* was to make it salient, usable and acceptable as a technology, so that users would actually want to use it. To accomplish this, we aimed to make the designs understandable at first glance. We also aimed to make it non-intrusive, such that users could get information from it without disrupting their broadcasts. One way in which we sought to minimize intrusiveness was to only have the nudging notify the broadcaster about location viewers within his or her current city; this would reduce the total number of notifications and limit them to only the most relevant information.

To achieve our design goals, we incorporated the following principles as design guidelines for our proposal designs of LVF: studies about pictograms also called "*Privacy icons*" ("simplified pictures expressing privacy-related statements") (Holtz et al., 2010), "icon language" (*rules of creating/designing icons to deliver the message*), as well as "icon requirements of widespread usage" highlighting the argument related to privacy implications, that is "The design should not obscure the nature and extent of a system's potential or actual disclosure" (Hansen, 2009). Each of these principles is discussed in detail below.

Existing research on pictograms, also "privacy icons", informed our design process. In general, pictograms are communication tools that visually deliver privacy statements to the users, rather than doing so via textual privacy policy statements (Lillebo, 2011). For example, Privacy Seals that are granted by a seal authority to retailers through a seal-of-approval program (Jensen and Potts, 2004; Lillebo, 2011). This seal indicates that the owner of the retail website is following the standard rules for protecting customers' privacy. For example, TRUSTe is a

privacy seal indicating that a website is safe to use by kids (Jensen and Potts, 2004; Lillebo, 2011) (Figure 4.1). Holtz at el. (2010) defined four areas in which “Privacy icons” can be used. One of which is to represent how personal information is used by others (Holtz at el., 2010; Lillebo, 2011). For example, Bickersta proposed the concept of “*Privacy Commons*”, “an icon set tailored to users in social networks ...” that uses privacy icons as a second layer among three layers (between a layer of full textual policy and a machine readable layer to be used for search engine) (Lillebo, 2011; Bickersta, 2009; Holtz at el., 2010). As Bickersta states, these privacy icons should be understandable from the user’s perspective (Bickersta, 2009). Specific criteria for privacy icon design, adapted from Lillebo (2011), are shown below.

- Icons should be easily understandable, regardless of cultural and social background, as well as age and level of education.
- Icons should provide information in a clear, easy-to-process way.
- Icons should be designed as circles rather than triangles, as triangles are strongly associated with warning and alarm.
- Likewise, icons should typically avoid colors like red, orange, and, yellow, which are associated with warning and danger (Edworthy, 1996); however, here we used such colors to underline the danger associated with the information being provided, and for the purpose of awareness.



Figure 4.1 The Privacy Seal Icon for the TRUSTe Granting Authority. Figure from (Lillebo, 2011)

Our design was also informed by the principles of icon language (Hansen, 2009). In particular, icon language would need “*Icon Alphabet*” (icons that are made of symbols, and parameters (e.g., number of broadcast viewers in our study case)). It would also need “*Icon language grammar*” that should be valid, such that the combination of symbols follows rules of

syntax. Icons should make sense both independently and in combination with other icons. Overall, the meaning of the icons should be easily processed, whether alone or when combined. The most critical requirement of designing icons is that “The design should not obscure the nature and extent of a system’s potential or actual disclosure”. Also, icons themselves should be simple, so that the design itself does not get in the way of conveying information. Icons should be chosen carefully in terms of the information they are representing, and should be understandable in combination. (Hansen, 2009).

We first established the icon language, and then used that as the basis for designing three prototypes. It should be noted that the icon language itself is not shown to the broadcaster; it was used only for the purpose of designing the icons. Each of the three prototypes is discussed below.

#### 4.1.2 Design 1: GeoLocate (GL) Prototype

The GL icon (Figure 4.2) shows broadcasters a number of different types of information, including an indicator of their own location (where they are currently broadcasting) (1 in the Figure 4.2 below), whether there are people viewing one’s location (2), the number of people viewing it (as a parameter) (3), the city of those viewing it, where the user is currently broadcasting (as a parameter) (4). Clicking on the GL icon (2) results in a viewable list of the particular viewers of the broadcaster’s location, with information for those viewers (Figure 4.3). Note: photos representing viewers taken from Google Image.



Figure 4.2 GeoLocate Icon

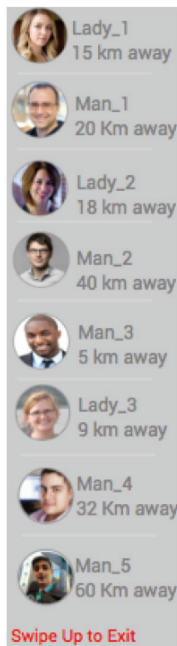


Figure 4.3 A List of Viewers Who are Viewing the Broadcaster’s Location.

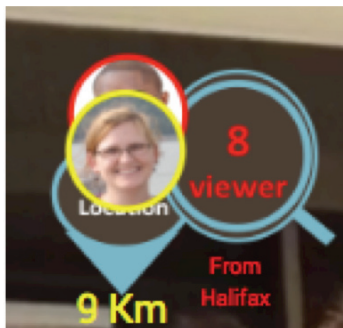


Figure 4.4 Circular Sliding Icons are Representing Viewers Who are Viewing the Broadcaster’s Location and are Moving Toward him

GL prototype also provides information on location viewers that are moving towards the broadcaster’s location. Figure 4.4 shows circular sliding icons that originate from the Find icon and represent the subset of viewers that are moving in the broadcaster’s direction (as indicated

by the movement towards the My Location icon). The display also shows the current distance between the viewer and the broadcaster's location; this changes dynamically to reflect movement by the location viewer. Note: photos representing viewers taken from Google Image.

***Icon Language Grammar (Syntax of symbols combination):***

1. There are (number of) viewers who are viewing my location and they are from Halifax (Figure 4.2).
2. Some of these viewers moving toward my location (Figure 4.4).

This is applied only when some of viewers moving toward your location.

***The Functionality of the Prototype***

Figure 4.5 demonstrates the functionality of this prototype. When the broadcast begins, the icon is hidden; it remains hidden until one or more viewers view the broadcaster's location. Starting at that point, the notification icon repeatedly grows and shrinks, representing the number of viewers who are examining the location of the broadcaster. An additional circular icon is sliding and flashing when a viewer within a set distance is approaching the broadcaster. Clicking on the 'GL' icon provides a list of viewers, including their usernames, their account profile's photo, and their distance from the broadcaster. Note: photos representing viewers taken from Google Image.



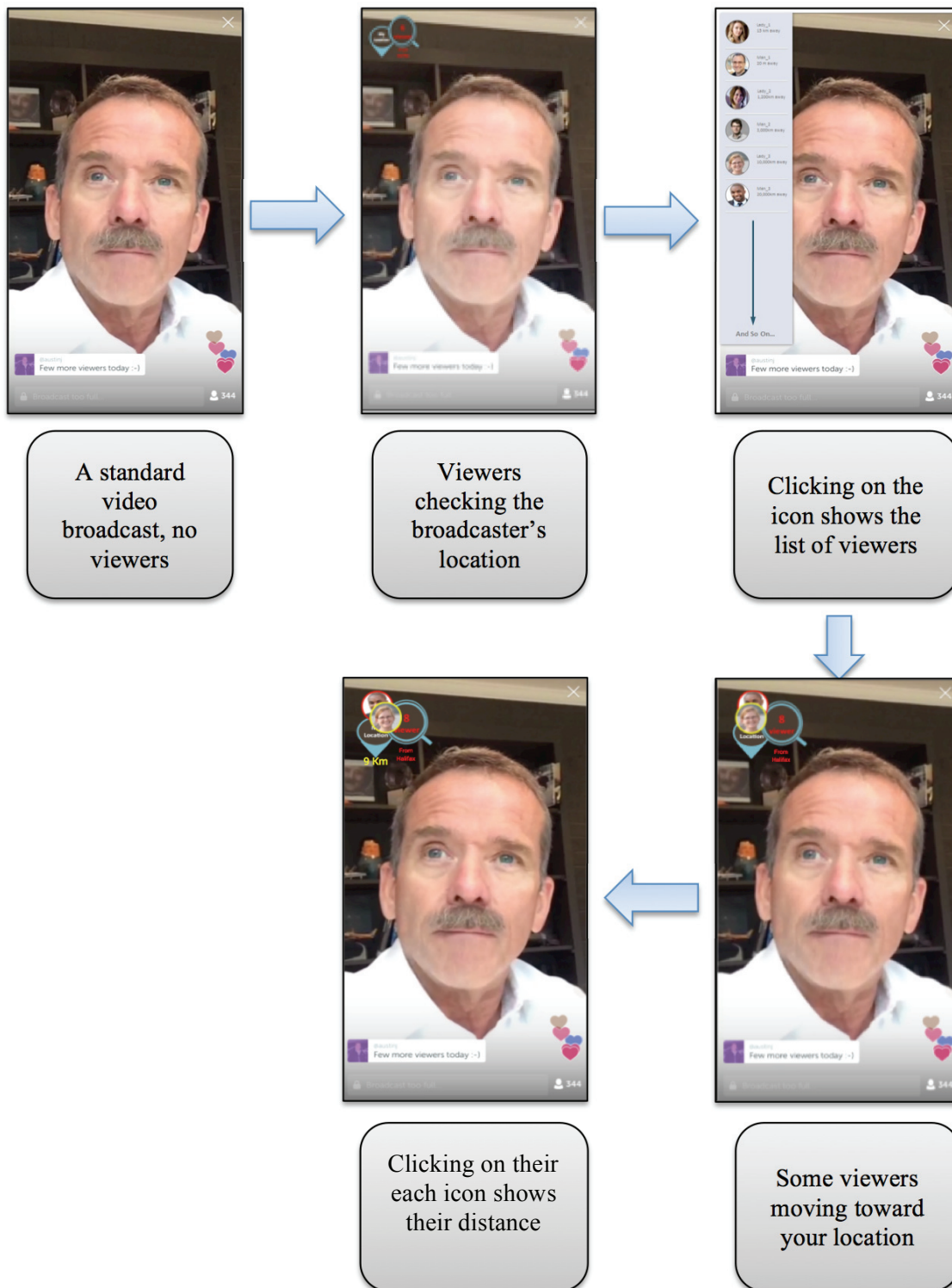


Figure 4.5 The Functionality of GeoLocate Prototype. The photo representing the broadcaster taken from (SiteSell Blog, 2015)

### 4.1.3 Design 2: GeoWatch (GW) Prototype

The GW icon is shown in Figure 4.6. It features a red eye that acts as a metaphor notifying the broadcaster that viewers are viewing the broadcaster's location (1 in Figure 4.6); when there are no such viewers, the eye is grey and crossed out (Figure 4.7). The icon also shows the number of location viewers (as a parameter) that are in the same city as the broadcaster (2 in Figure 4.6). "My Location" icon (3) is representing the broadcaster's location. Clicking on GW icon provides a radar plot that shows the location viewers and their information (Figure 4.8).



Figure 4.6 GeoWatch Icon



Figure 4.7 GeoWatch Icon (Inactive Mode)

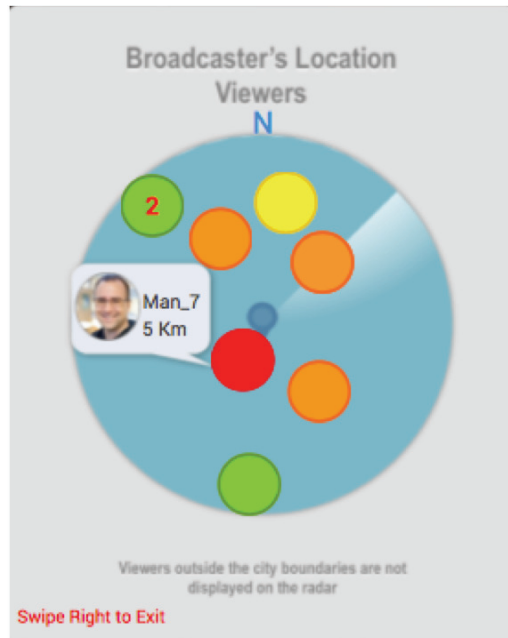


Figure 4.8 A Radar Plot Showing the Location of Viewers Who are Checking the Broadcaster’s Location.

This prototype also features a radar plot that automatically updates the location of viewers who are viewing the location of the broadcaster, dynamically showing their movement in relation to the broadcaster. Geographic orientation is indicated by the letter “N” (north). Color coding is used to visually indicate the level of danger based on distance from the broadcaster: red for 5 km or less, orange for 6-15 km, yellow for 16-25 km, and green for more than 25 km. The color of the circles, representing particular viewers, will change to represent changing distance from the broadcaster (e.g., green to yellow as they get closer). Note: the photo representing a viewer taken from Google Image.

***Icon Language Grammar: (Syntax of symbols combination):***

1. There are viewers watching my location (Figure 4.6).

The eye metaphor was adopted from Zhou (2015) who used it to notify a mobile phone user about people who are watching his/her mobile’s content through shoulder surfing. In addition, it is the symbol that Snapchat app uses to show the user about people who view the user’s snaps (picture or video).


The combination of the eye metaphor and “My location” symbol represent that there are

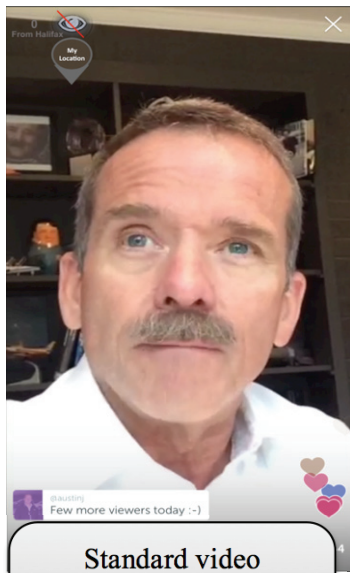
viewers watching my location (the broadcaster's location). On the left of the eye metaphor is the parameters, which illustrate how many viewers watching the location and the city where they are located and where the broadcast is taking place.

## 2. No viewers are watching my location. (Figure 4.7)

The combination of the red line that is canceling the eye metaphor, and the "My location" symbol represent that no one is watching my location (the broadcaster's location). The parameter of the canceled eye is number zero and the city confirm that no one is watching my location from the city where the broadcast is taking place.

### ***The Functionality of the Prototype***

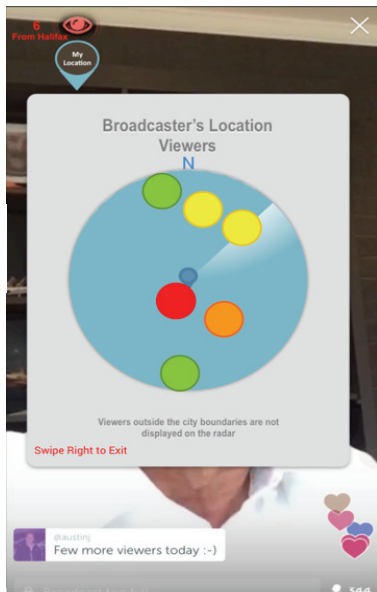
The functionality of the prototype is shown in Figure 4.9. At the start of a broadcast the inactive GW icon (Figure 4.7) is displayed. When viewers start checking the broadcaster's location, the icon switches to active mode. If the icon is clicked, the radar plot is displayed to show all location viewers within a set distance. Clicking any individual circle on the radar reveals that viewer's username, profile photo, and actual distance from the broadcaster. Compared to the first prototype, this one is more intrusive because the radar map blocks out the broadcast; however, it provides a better spatial map. When a particular viewer has just started to view a broadcaster's location, the circle on the radar plot appears suddenly and bounces for few seconds, then remains stable. When the viewer stopped watching the broadcast, the circle disappears. If there are two viewers located approximately at the same location, then the circle will contain the number of viewers located there. Clicking on that circle will display their information in sequence. Moreover, when a viewer starts getting closer to the broadcaster's location, the circle object (represent the viewer) dynamically moves toward the location symbol . When the viewer is getting further from the broadcaster's location, the circle object moves away from the location symbol. In addition, the viewer may be moving in and out from the broadcaster's location, such that the circle object passes the location symbol. For all movement types, whether related to movement by the broadcaster or by the location viewer, the color-coding of the circle object is changing according to the associated distance. To exit from the radar plot interface, the broadcaster has to swipe right at the bottom of that interface (Figure 4.8).



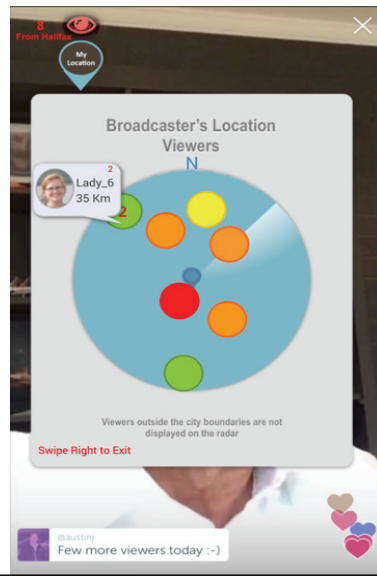
Standard video broadcast, no viewers watching the broadcaster's location



The icon is activated once viewers are checking the location



Clicking on the GeoWatch Icon provides a radar plot of location viewers



A circle including the number of viewers who are located at that location, clicking on each circle shows the viewers' information

Figure 4.9 The Functionality of GeoWatch Prototype. The photo representing the broadcaster taken from (SiteSell Blog, 2015)

### 4.1.4 Design 3: GeoBar (GB) Prototype

The third prototype GB, shown in Figure 4.10, displays similar information but is laid out differently than the first two. The prototype shows profile photos for those people viewing the broadcaster's location (1 in Figure 4.10), as well as the city of the viewers and how many of them there are (2). The display also indicates the distance of the viewers (3) from the broadcaster, which is represented by the "My location" icon (4). In contrast to the radar plot, this representation of distance is less informative because it does not specify direction; however, it is also less intrusive. Note: portraits taken from Google Image.

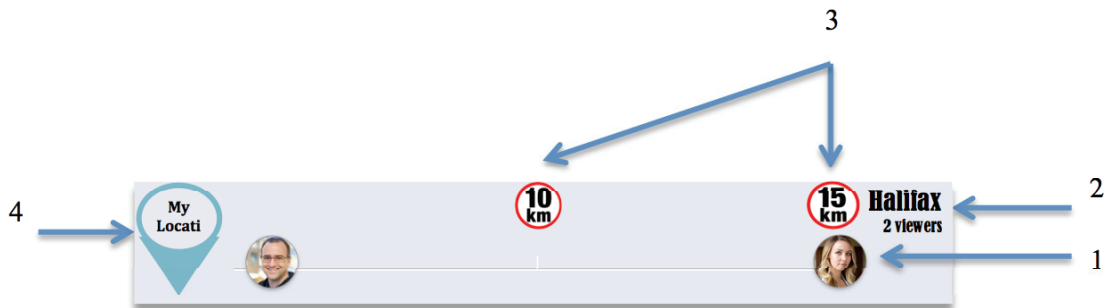


Figure 4.10 GeoBar Graphical Representation

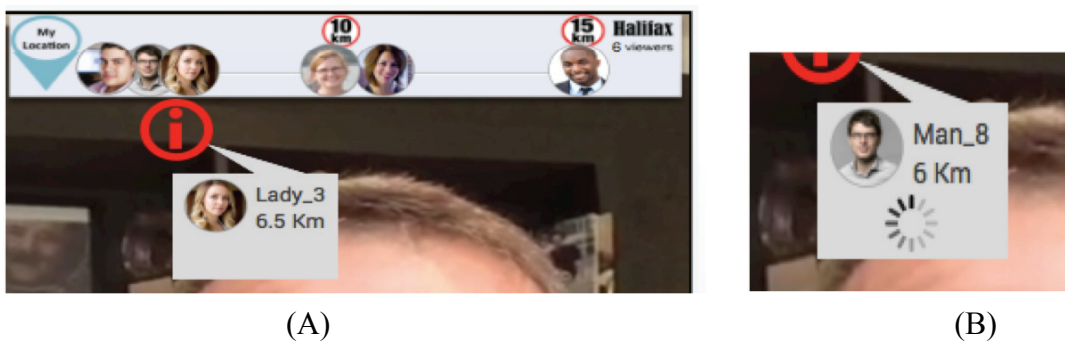


Figure 4.11 (i) icon is shown only when two viewers or more located at the same location

### ***The Functionality of the Prototype***

Figure 4.12 demonstrates how the GB prototype works. It is displayed by default once the user starts broadcasting, visible even if there are no location viewers. When viewers located within 15 km of the broadcaster start viewing the broadcaster's location, their profile photos suddenly appear on the bar. Clicking on their profile photos provides their information, including username and distance from the broadcaster. Like the other prototypes, this one will actively show changes in proximity via moving profile photo. When a viewer stops viewing the broadcaster's location, the corresponding profile photo disappears. When two or more viewers have approximately the same location, an icon flashes (Figure 4.11). Clicking on this icon causes the information about these viewers to be displayed in sequence starting with the information of the closer viewer to the broadcaster's location. Note: photos representing viewers taken from Google Image.

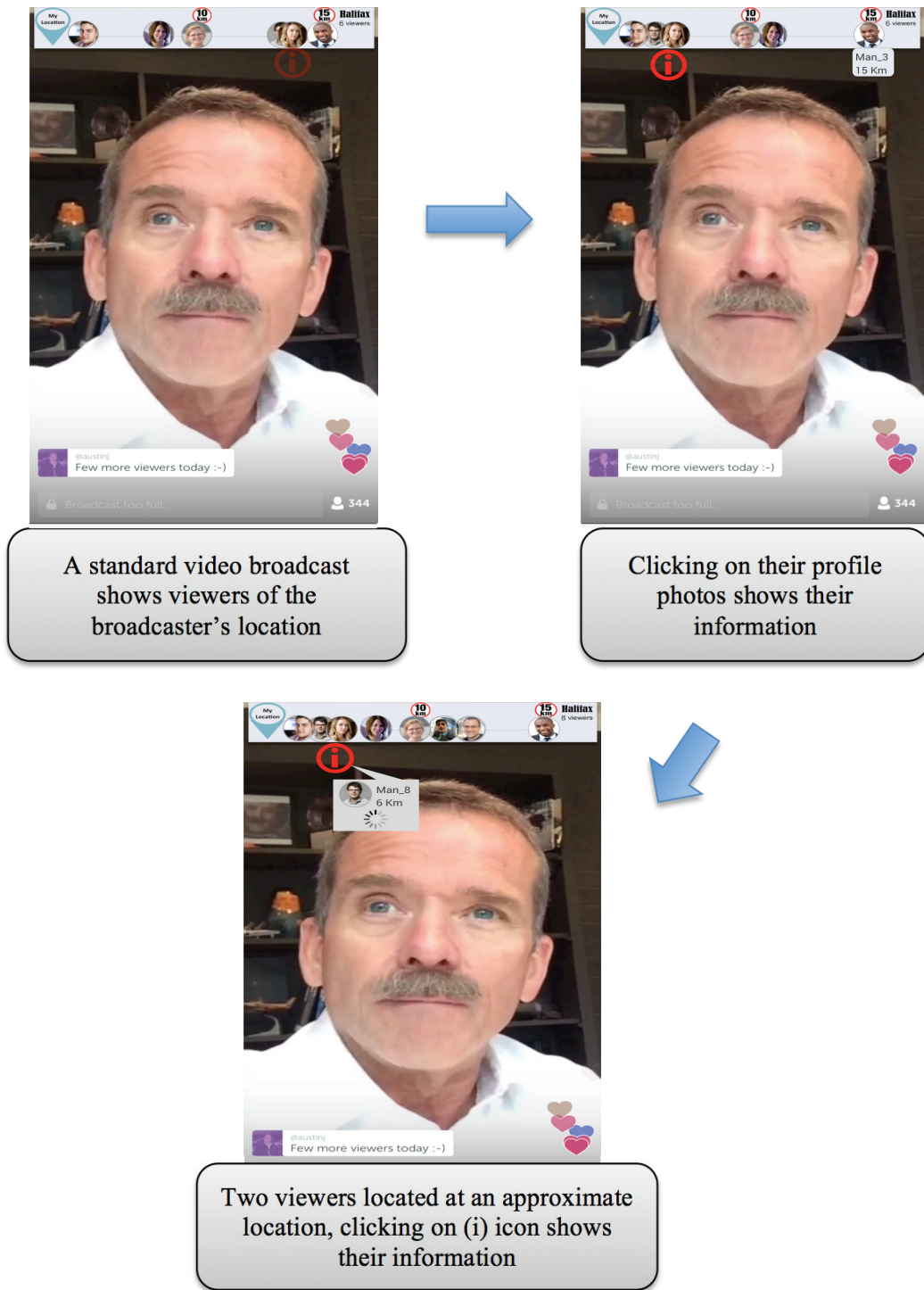


Figure 4.12 The Functionality of GeoBar Prototype. The photo representing the broadcaster taken from (SiteSell Blog, 2015)



## 4.2 Visual Privacy Awareness Prototypes (VPAPs)

### 4.2.1 Theoretical Foundation:

To find a solution for the visual privacy issues reported in our survey results and often observed on live video broadcasting apps, we first sought to determine which kinds of social media posts have been most regretted by users. Due to the lack of research on live video broadcasting apps, we found that Facebook, with its generic social media functionalities (e.g., the ability of creating posts of text, pictures and videos), served as the best starting point. Users typically regret posts that contain sensitive content, including personal and family issues, religious and politics opinions, negative or offensive comments, complaints about work and companies, sex-related content, and content related to alcohol or drug use (Wang et al., 2011). Wang et al. (2011) also addressed how and why these posts become regrets, and found that these posts often result in unforeseen consequences (e.g., unintended audience), usability problems and unfamiliarity with or misunderstanding of social media network. We specifically sought out research related to Snapchat use, because it is the first temporal social media app, and found that they do send sensitive content. A Study with 127 Snapchat users reported that about 45% of respondents had sent content while drunk, 23% had engaged in Joke sexting “in which sexual or pseudo- sexual content is sent as a joke”, and 12% had engaged in sexting (Roesner, Gill & Kohno, 2014). In YouTube-related research, we found the phenomena of Card Stories (see Section 2.3.2) and concluded that this phenomenon is common with users who have experienced negative personal issues associated with negative emotions (e.g., depression).

Based on our observation of live video broadcasting, we found two common broadcaster activities that may result in negative consequences: talking about personal issues and broadcasting under the influence of alcohol or drug use. These types of activities are common types of posts that are either a user could regret about later (and that originated from negative mood, or show self-disclosure behavior that originated from positive or negative mood). However, some users have their own strategies for sharing information to handle the possibility of regrettable posts. For example, some Facebook users delay posts to be sent until a later time in order to decide whether or not to post it; others use fake names or use multiple accounts, while some users delete posts after posting or apologize for negative posts. Other strategies involve

declining or ignoring friend requests and using privacy settings. However, not all of these strategies are applicable to live video broadcasting. In the case of the Card Stories phenomenon on YouTube (see Section 2.3.2), some users tell their stories without revealing their faces, instead pointing the camera at the story cards. A similar strategy observed with live video broadcasting is the wearing of a mask during broadcasting. Similarly, broadcasters sometimes pointed the camera at a wall or floor – anywhere but the broadcaster him or herself. These tactics highlight the need for visual privacy in live broadcasting.

Based on the privacy concerns outlined earlier, as well as these observations of how people try to protect their visual privacy, we propose visual privacy awareness mechanisms intended to protect the visual privacy of live video broadcasters. In light of the documented circumstances in which regrettable posting most often occurs, we aim to improve visual privacy specifically for those in negative moods and those under the influence of alcohol.

To address visual privacy in those under the influence of alcohol, we had to be able to detect users who met that criterion. Our efforts were informed by the task-based tests used in real life. In particular, police officers test suspected drunk drivers using the Standard Field Sobriety Test, which involves three examinations: horizontal gaze, walk-and-turn, and the one-leg stand (AAA DUI Justice Link, para. 1). In 2008, Gmail launched a service that operates on the same principle to prevent drunk emails: the user must solve easy math problems before clicking on ‘Send’. Likewise, several apps have been developed to prevent drunken people from posting on social media sites. These apps used a social media sobriety test implemented by the Web security firm Webroot via software that enables the user to select the social media site and the time during which he or she wants to be kept out (Dailymail, 2010). When the user visits the social media site, the social media sobriety test requires the user to perform a variety of tasks: ‘drag your mouse in a straight line’, ‘type the alphabet backwards’, or ‘follow the finger.’ If the user successfully completes the tasks, then he/she can post. If not, then the social media sobriety test prevents them from posting, and it posts “too drunk to post right now”. However, these apps, and the social media sobriety test, are no longer available. These tasks were designed specifically for drunk people. In our work, we aim to include drunk people as well people in specific moods, whether negative or positive.

Our goal is to alert broadcasters who are in atypical moods of potential privacy self-disclosure behavior consequences, and to increase visual privacy. To achieve this goal we also

used the concept of privacy nudge, which is a soft paternalism solution to the problem. The idea behind soft paternalism is to help the user make informed decisions. The system that is used this approach targets to enhance or affect user behavior (Acquisti, 2012). In the case of this study, we do not prevent a user from broadcasting, which is considered strong paternalism; instead, we show clues to the user so that they might reconsider their behavior and make a decision on that basis. In doing so, we aim to reduce the possibility of self-disclosure behavior for drunk people and protect their visual privacy. We intend to provide similar protection for those in negative moods (e.g., depressed or angry), as well.

With respect to privacy awareness design, the “*malleability* of privacy preferences” refers to “the observations that ... various factors can be used to activate or suppress privacy concerns, which in turn affect behavior” (Acquisti et al., 2015). One of these factors is the default setting that affects information disclosure (Acquisti et al., 2015), and privacy self-disclosure behavior. Moreover, the use of “*malicious interface design*” is another factor that refers to designing “features that frustrate or confuse the user into disclosing personal information”. We consider these two tools to apply the soft paternalism in our proposal designs. Our design features are two stages: the first works as a detection for those who are drunk or in atypical moods, while the second is a response (in form of protection) and awareness stage.

As a framework for our prototype design, the first stage, detection, is task-based. We used the Design with Intent (DwI) method as guidance for designing a task that serves as a testing process and a mechanism to influence user behavior. DwI means “design that is intended to influence or result in certain user behavior” (Lockton et al., 2010). It includes lenses (“a way of grouping design patterns which share similar considerations, behavioral understanding or assumptions about how to influence users” (Lockton et al., 2010), and each lens contains patterns for influencing behavior through design (Lockton et al., 2010). The second stage is protection, which involves a response to a user choice, possibly leading to a higher level of visual privacy, depending on the user’s choice. To provide flexibility, we also provide user control over the visual protection, with added alerts related to protection in the case of opting out. On the basis of these principles, we propose three task-based prototypes: ‘Matching mood-to-mood’ task, ‘Matching your appearance-to-mood’ task, and ‘Choosing your appearance directly’ task. For all three prototypes, we were inspired by the *Errorproofing Lens* from DwI, which treats the target behavior as an error (Lockton et al., 2010, p. 21); the design is therefore intended to help

the user to avoid it (Acquisti et al., 2015). In the present context, the target behavior is showing one's appearance while broadcasting. We treated that behavior as an error for people who are broadcasting in an atypical mood, with the aim of protecting their visual privacy. Specifically, we used the pattern "*Task lock-in/out*", which refers to "Can you keep a task going that needs to be, or prevent one being started inadvertently?"(Lockton et al., 2010, p. 31). In the context of this study, this means that broadcasting would not start unless the user does the task. Therefore, we proposed that once the broadcaster clicks the broadcast starting button, the task by default is shown up to the user before even broadcasting. Another lens we adopted is the *Architectural Lens*, which indicates how that structure of the system is designed to influence user behavior (Lockton et al., 2010, p. 8). This refers to the basic functionality or the framework of our proposal prototype, as described in the beginning of this section. We considered the pattern "*Simplicity*": "How simply can you structure things, to make it easier for users to do what you would like them to do" (Lockton et al., 2010, p. 20). Thus, our objective was to make the structure simple and easy.

The following section elaborates how we designed each prototype, with a focus on the two stages described above, detection and protection.

#### **4.2.2 Matching Mood-to-Mood Task (MMT)**

The task is used in the testing process to detect mood, but could also influence user behavior when making the user aware of potential issues of visual appearance.

##### ***Overview of the functionality of the prototype:***

The task requires the broadcaster to swipe their current mood metaphor to the appropriate exact mood metaphor. Depending on the user's choice, the app will set to the default setting of a higher level of visual privacy, either blurring or hiding the broadcaster's appearance: if the match is imperfect or the mood is not happy, then the app will be set to that higher level of visual privacy. For example, if the user swipes the happy triangle to the perfect happy triangle, then the app will explicitly display the user's appearance, foregoing the higher security level. In contrast, if the user swipes the happy triangle to the bent happy triangle, then the app will either blur or

hide the user's appearance. As another example, if the user swipes the drunk square to either the perfect or the bent drunk square, then the app will be set to the higher level of visual privacy. The same will happen with the angry and depressed symbols. The broadcaster has the control to reveal, blur or hide their appearance by clicking on the "filter" icon (Figures 4.13 and 4.14).

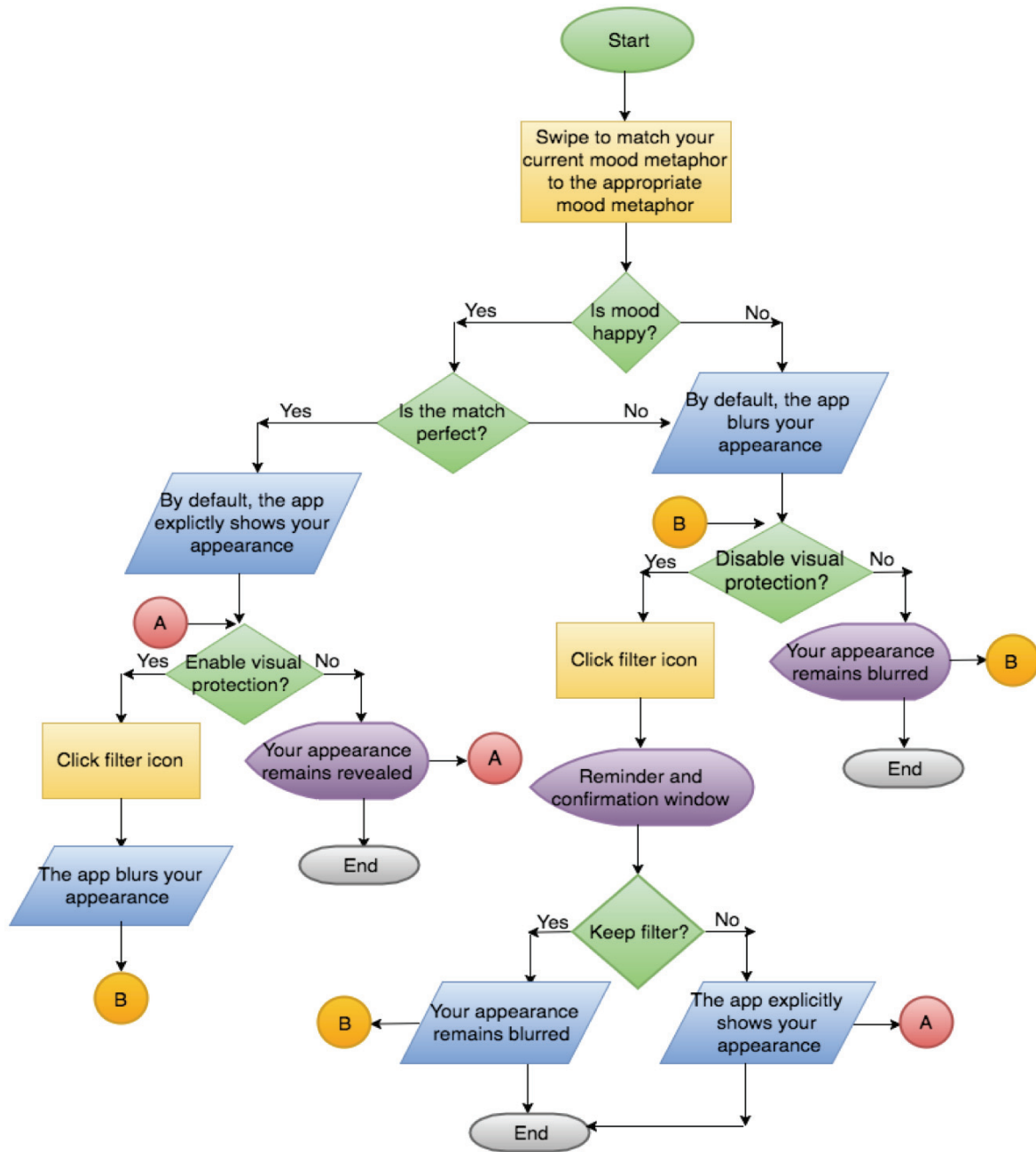


Figure 4.13 Flowchart of Mood-to-Mood Task Functionality. (A): The point where you can enable visual protection. (B): The point where you can disable visual protection.

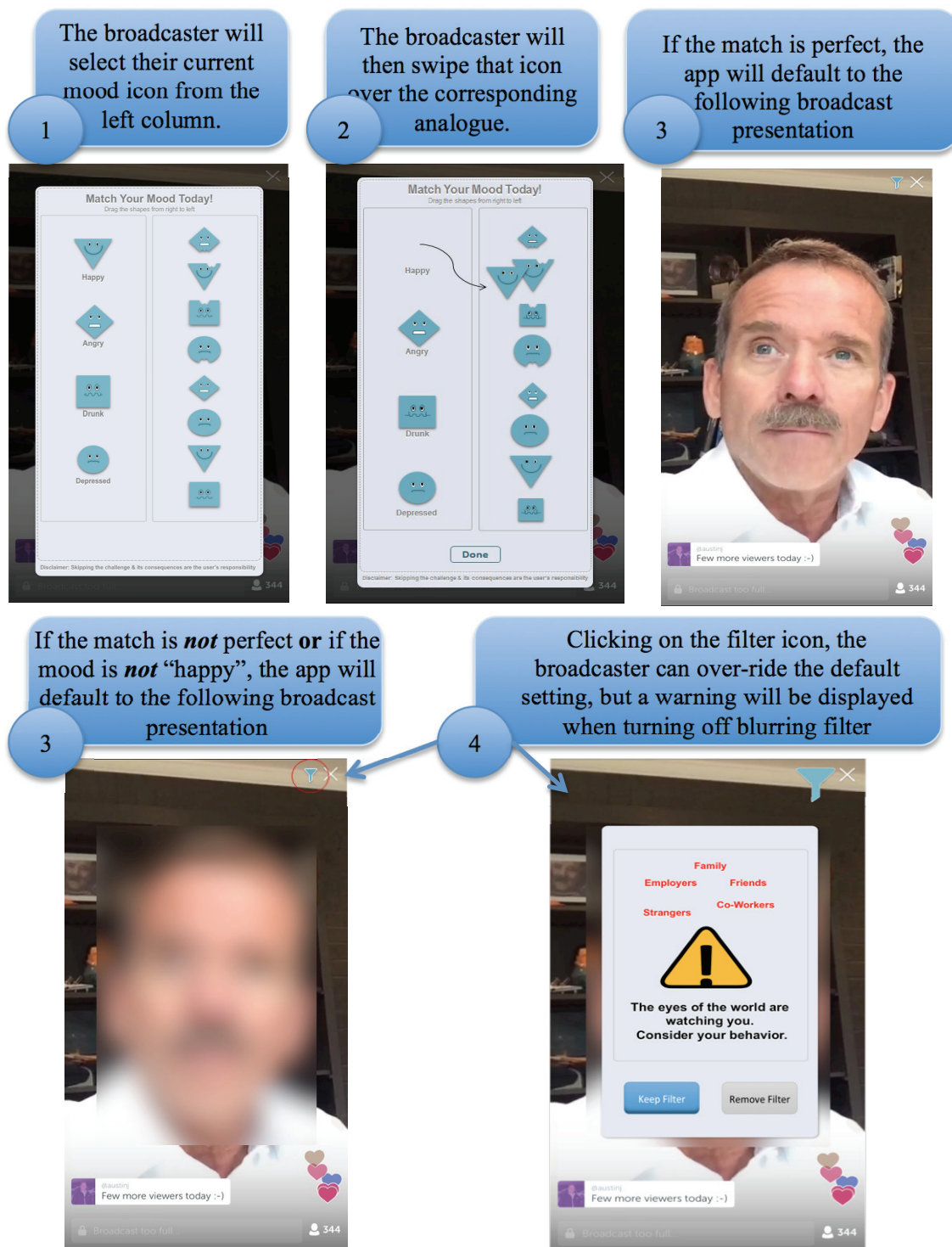


Figure 4.14 Mood-to-Mood prototype: The Case of Matching Happy Mood. The photo representing the broadcaster taken from (SiteSell Blog, 2015)

The design components of MMT prototype are discussed below

### ***Task Interface***

#### **The interface design of the task built according to Dwl lenses and patterns as following:**

1. *Errorproofing Lens*: Considering people's unconscious behavior in our design, we took advantage of the *Errorproofing Lens* (see Section 4.2.1). We obtained the general idea of the task type from the pattern "*Matched Affordance*," which is "Can you make parts fit only when the right way round, or only with the products they should do?" (Lockton et al., 2010, p. 28). From this pattern we decided to make a matching shape-based task that would be difficult for broadcasters who are under the influence of alcohol to solve correctly. On the other hand, it would be easily solvable for non-drunk broadcasters.

2. *Perceptual Lens*: This addresses "how users perceive patterns and meaning as they interact with the system" (Lockton et al., 2010, p. 55). It uses semantics, semiotics, and is applied by graphics. We adopted the pattern "*Mood*": "Can you use color images or other sensory stimuli to set a particular mood for a user's interaction with your system?" (Lockton et al., 2010, p. 63) to apply this pattern, we first specified which moods can be included. We adopted some the examples of mood that were presented in a survey about regretted posts (Wang et al., 2011): "depressed", "angry", and "happy." We added "drunk" for the MMT. To design these moods, we applied the pattern "*Metaphors*": "Can you employ a metaphor/analogy of something familiar, so people understand or use your system the same way?" (Lockton et al., 2010, p. 61) (Figure 4.15). We also applied the pattern "*(A) symmetry*": "Can you use symmetry to make elements look related, or asymmetry to show difference and focus attention?" (Lockton et al., 2010, p. 56). We used this pattern for the purpose of detecting drunk people. Therefore, for each mood metaphor (Figure 4.15), we made an equivalent imperfect metaphor by altering their appearance (Figure 4.16).





Figure 4.15 Metaphors of Moods Used for Task-Based Awareness Design

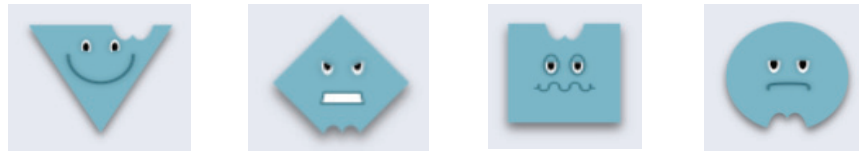


Figure 4.16 Imperfect Metaphors for the Purpose of Detecting Drunk People

3. *Cognitive Lens*: This is used for behavioral economics and cognitive psychology research. It focuses on how people make decisions, and how decision-making is affected by experience (Lockton et al., 2010, p. 73). We applied the “*Emotional Engagement*” pattern: “Can you design your system to engage people’s emotions, or make them emotionally connected to their behavior?” (Lockton et al., 2010, p. 79). The title of the task, “Match your mood today”, and the mood metaphors are clues of how to solve the task and a way of getting them to engage in expressing their current feelings and mood, which is of particular importance since most frequent users use social media for psychological reasons (Correa, Hinsley and De Zuniga, 2010). Setting a visual privacy based on the user’s choice is a privacy management rule that varies based on situation, culture, and motivation, and that the effect of that privacy rule are learned over time (Acquisti et al., 2015). It could also shape the user’s behavior in terms of broadcasting while the user is experiencing negative mood (Figure 4.17).

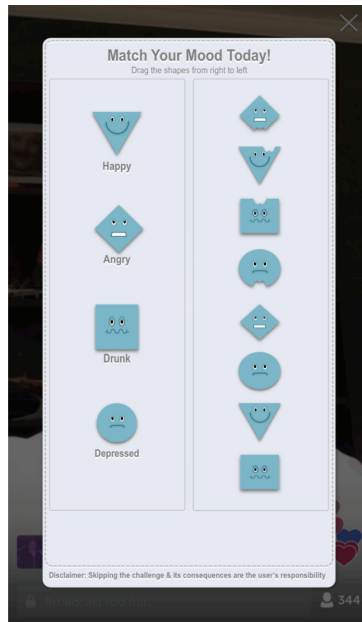



Figure 4.17 The Interface of Mood-to-Mood Task

### ***Response Stage***

1. From Errorproofing Lens, we used the pattern “*Defaults*”: “Can you make the default setting the behavior you would prefer users to perform?” (Lockton et al., 2010, p. 25). We made the blurring filter or inpainting (hiding) as the default visual privacy setting for those who performed a certain way on the task, which is imperfect matching or choosing the moods that are not happy.

### ***User Control***

1. We used the “Filter” icon  to enable the user controlling the visual privacy setting to either show (turning off the filter) or conceal their appearance. From the Errorproofing Lens, the pattern “*Are you sure?*”: “Can you design an extra ‘confirmation’ step before an action can be performed” (Lockton et al., 2010, p. 22) was applied in the form of a window. The whole window is inspired by the “Interaction Lens”. We adopted the pattern “*Kairos*”: “Can you give users a suggestion at exactly the right moment for them to change their behavior?” (Lockton et al., 2010, p. 34). We used this pattern for the moment when the broadcaster wants to turn off the blurring or hiding mechanisms

(Figure 4.18). This window is formed according to three patterns in combination. The first part is at the top of the window, using “Security Lens”: “aims to detect and prevent unwanted behavior” (Lockton et al., 2010, p. 104) (i.e., “Peerveillance”: “What happens if users know (or believe) that what they are doing is visible to their peers also using the system?” (Lockton et al., 2010, p. 106), and Surveillance “What happens if users know (or believe) their behavior is visible to or monitored by people in positions of power/authority?” (Lockton et al., 2010, p. 108)) (Figure 4.18). The second part, which contains the warning, is designed according to the pattern “*Conditional Warning*”: “Can you give users warnings based on detecting the error they have made, or might be about to make?” (Lockton et al., 2010, p. 24) (Figure 4.18). In the third part, we also applied the “Kairos” for the option we suggested to the broadcaster to choose, making the color of the “Keep Filter” button blue as opposed to the gray color of the “Remove Filter” that we do not suggest (Figure 4.18).

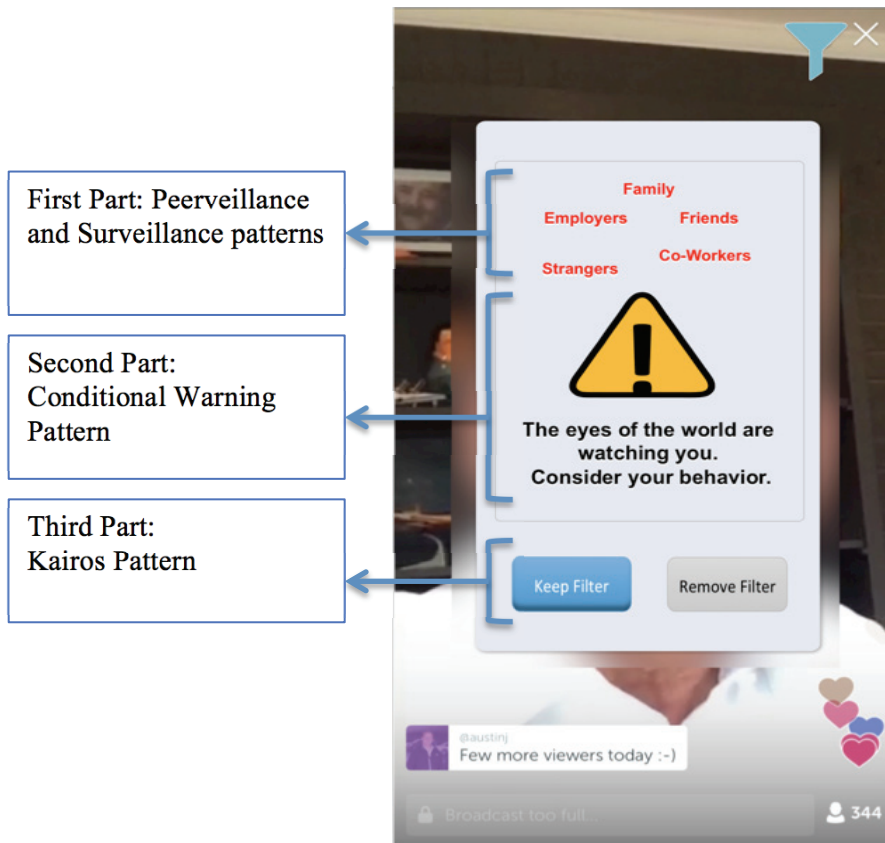


Figure 4.18 A Reminder and Confirmation Window Once Turning Visual Protection Off

### 4.2.3 Appearance-to-Mood Task (AMT)

The task is used in the testing process to detect mood, but could also influence user behavior when making the user aware of potential issues of visual appearance.

#### *Overview of the functionality of the prototype:*

The broadcaster has to swipe from one of two self-portraits (one blurred and one not) to one of five mood metaphors. One of the self-portrait is a standard live video and the other is a blurred live video. Depending on the user's choice, the app will set to default setting of higher level of visual privacy, either to blur or hide the broadcaster's appearance. If the selected self-portrait is standard and is swiped to the happy mood metaphor, then the app will explicitly shows the broadcaster's appearance. If the selected self-portrait is that standard and is swiped to any of the

other mood metaphors (e.g., angry, depressed, drunk, drunk and happy), then the app will be set to higher level of visual privacy (e.g., blurring or hiding the broadcaster's appearance). If the selected self-portrait is the blurred and is swiped to any of the mood metaphors, the app will also be set to higher level of visual privacy. The broadcaster has the control to reveal, blur or hide their appearance by clicking on the "filter" icon (Figures 4.19 and 4.20).

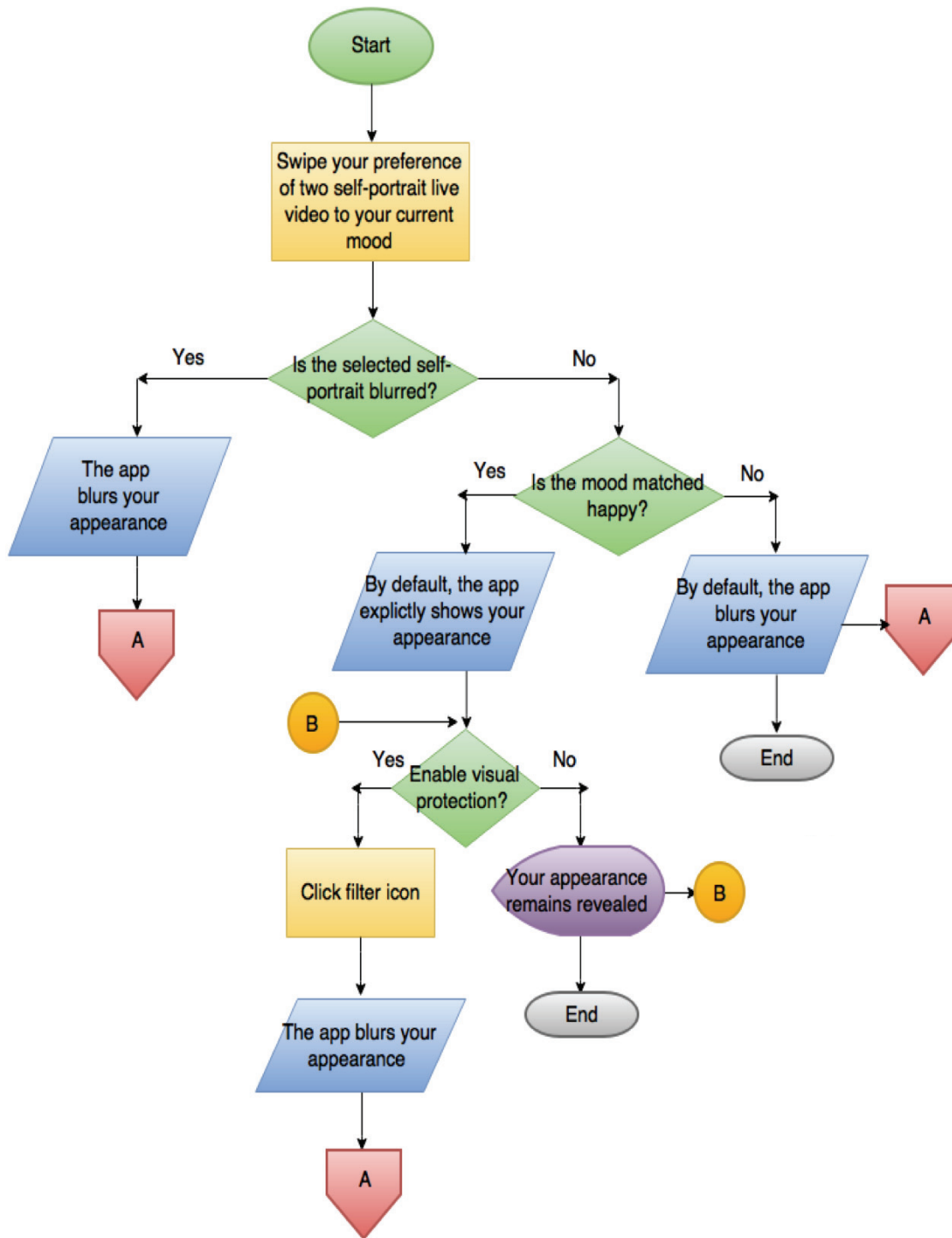


Figure 4.19 Flowchart of Appearance-to-Mood Task Functionality

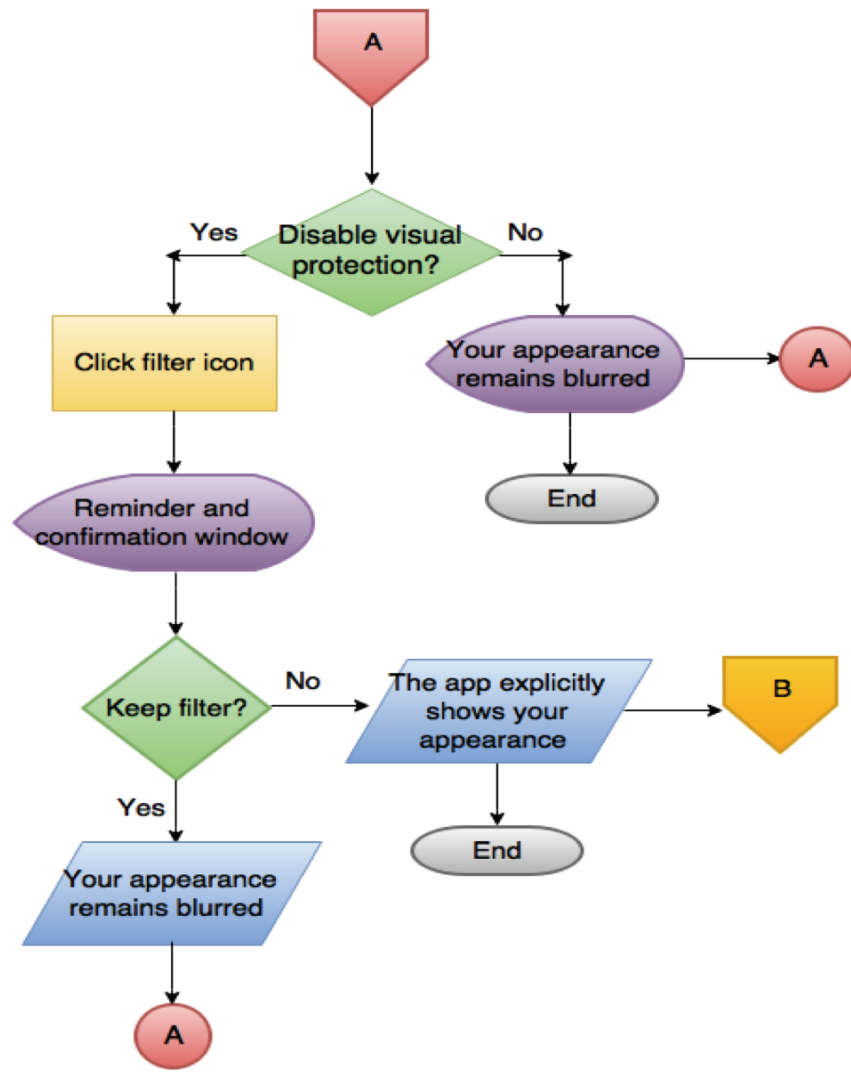
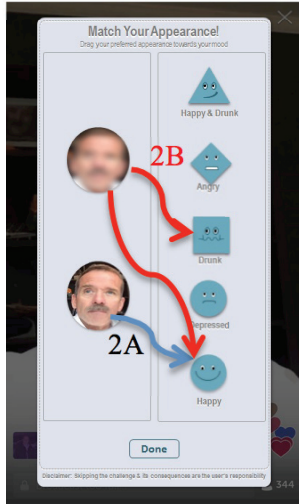


Figure 4.19 CONT. Flowchart of Appearance-to-Mood Task Functionality

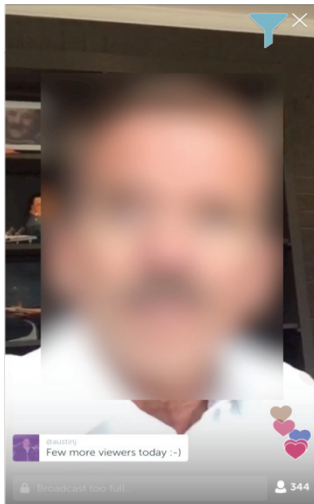
1 The broadcaster will swipe either the standard self-portrait live video or the blurred self- portrait live video to their current mood



2A If the standard self-portrait selected to match with happy mood, then the app explicitly shows appearance



2B If the blurred self-portrait selected to match with any mood, or the standard with unhappy mood, the app blurs appearance



3 Clicking on the filter icon, the broadcaster can over-ride the default setting, but a warning will be displayed when turning off blurring filter

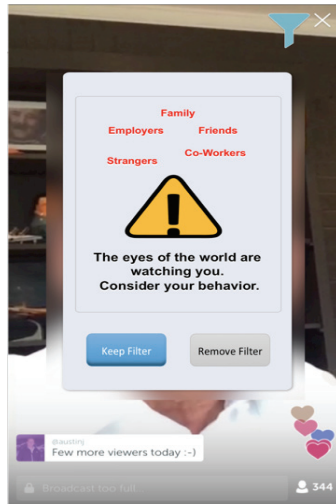


Figure 4.20 Appearance-to Mood Prototype. The photo representing the broadcaster taken from (SiteSell Blog, 2015)



## Task Interface

The interface design of the task built according to DWI lenses and patterns as following:

1. *Errorproofing Lens*. AMT and MMT are similar in that they are both matching-based tasks. So we adopted only the idea of matching from the pattern “*Matched Affordance*”.
2. *Perceptual Lens*: To form the matching task using “Mood” and “Metaphor” patterns, we designed one column that represents the type of moods, adding “happy and drunk” mood (Figure 4.21). The other column has two self-portraits of the actual broadcaster’s live video, used as a metaphor for the broadcaster’s appearance: one is blurred and one is not (Figure 4.22).



Figure 4.21 Metaphors of Moods for Appearance-to-Mood Task

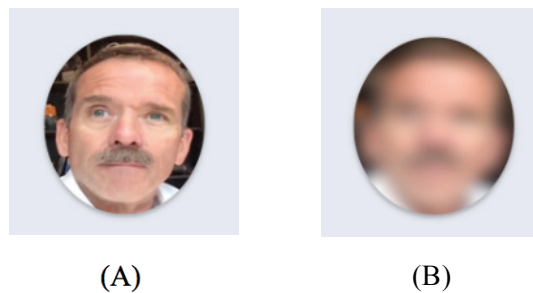


Figure 4.22 (A) A Standard Live Video, (B) A Blurred Live Video. The photo representing the broadcaster taken from (SiteSell Blog, 2015)

3. *Interaction Lens*: The patterns under this category collect the most common interface design elements that guide how the interaction with the system affects behavior (Lockton et al., 2010, p. 32). This includes patterns from Persuasive Technology, “where computer and phone affect behavior through contextual information and guidance”. We used the pattern “Simulation and feedword”: “Can you give users a preview or simulation of the results of different actions or choices?” (Lockton et al., 2010, p. 32). For this reason, we show the standard and blurred live video images as metaphors to provide an insight into how the broadcaster’s appearance would be for the corresponding match (Figure 4.23).

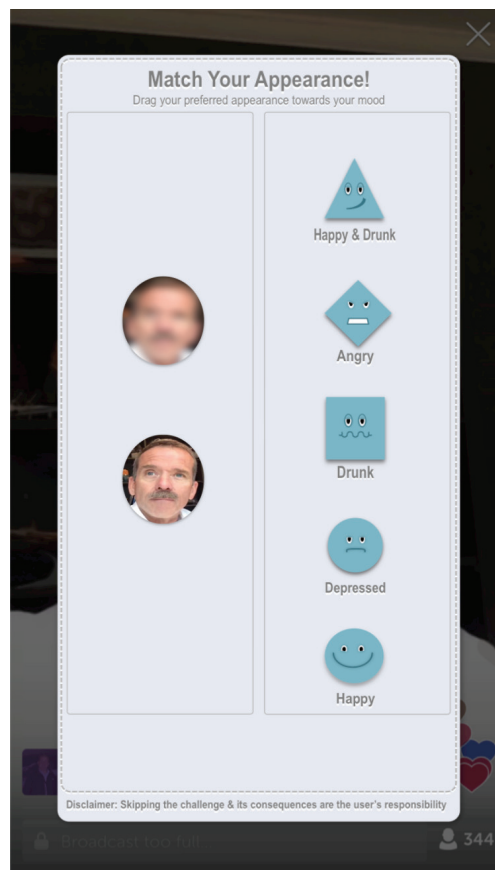


Figure 4.23 The interface of Appearance-to-Mood Task

### *Response Stage*

1. From Errorproofing Lens, we used the pattern “*Defaults*”：“Can you make the default setting the behavior you would prefer users to perform?” We set the blurring filter or inpainting (hiding) as the default visual privacy setting for the moods that are not happy and for the blurred self-portrait metaphor.

### ***User Control***

See Section User Control in 4.2.2.

## **4.2.4 Choosing Your Appearance Directly Task (ADT)**

The task is used in the testing process to detect mood, but could also influence user behavior when making the user aware of potential issues of visual appearance.

### ***Overview of the functionality of the prototype:***

This design reminds the broadcaster to consider their “obligation” to themselves, in terms of their family, friends, co-workers, and employers, as well as strangers. The broadcaster has to choose one of two self-portraits, one representing a blurred live video and the other representing a standard, unblurred one. The user’s choice will determine whether the higher level of security, with identity hidden or blurred, will be implemented. If the standard self-portrait is selected, the app will explicitly show the broadcaster’s appearance. If the blurred self-portrait is selected, then the app will be set to the higher level of visual privacy (i.e., blurring or hiding the broadcaster’s appearance). The broadcaster has the control to reveal, blur or hide their appearance by clicking on the “filter” icon (Figures 4.24 and 4.25).

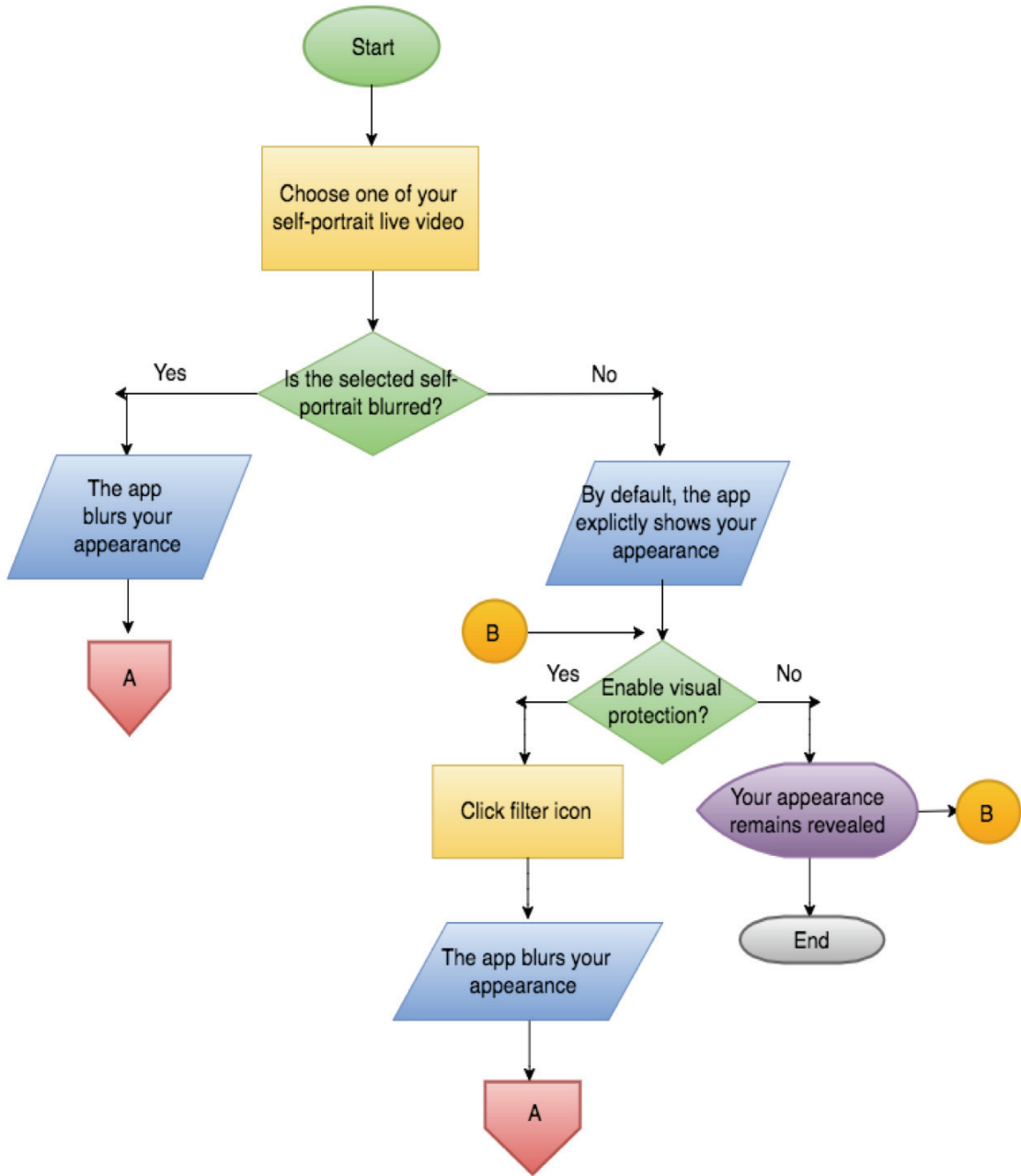


Figure 4.24 Flowchart of Choosing Your Appearance Directly Task

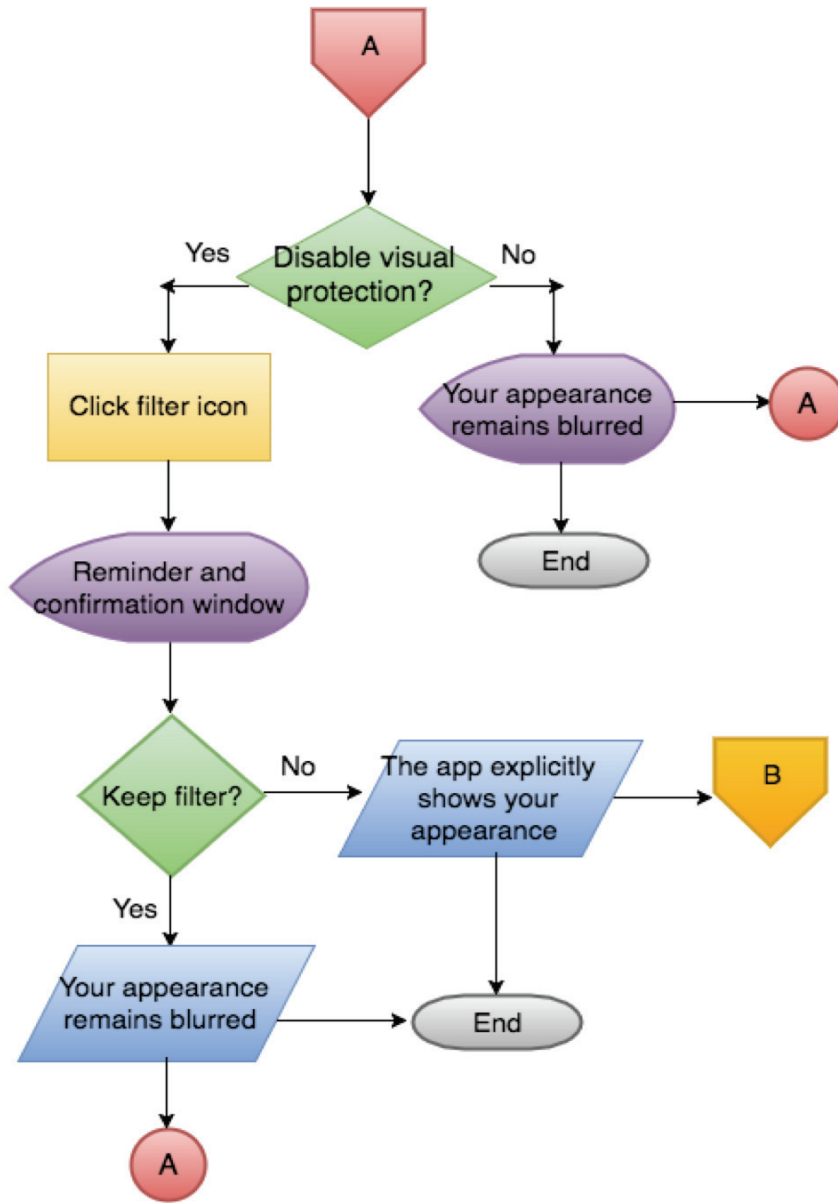


Figure 4.24 CONT. Flowchart of Choosing Your Appearance Directly Task

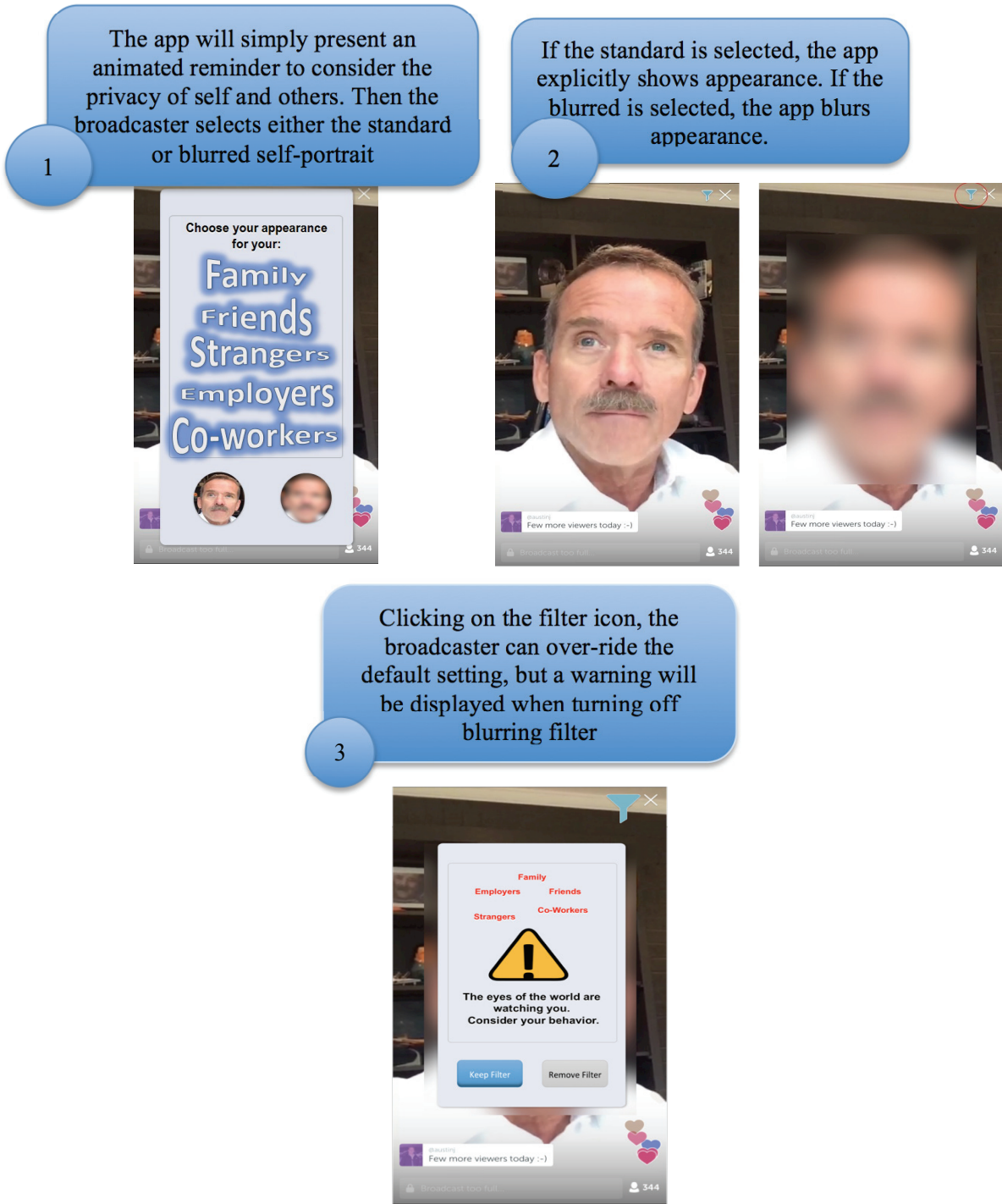


Figure 4.25 Choosing Your Appearance Directly Task Prototype. The photo representing the broadcaster taken from (SiteSell Blog, 2015)

## ***Task Interface***

**The interface design of the task built according to Dwl lenses and patterns as following:**

1. *Security Lens*: It aims to detect and prevent unwanted behavior (Lockton et al., 2010, p. 104). From the designer’s perspective, it seems unfriendly because it is “effectively treating users as guilty until proven innocent” (Lockton et al., 2010, p. 104); however, this can be designed in a way that the user can control their behavior to suit their needs. We adopted the pattern “*Peerveillance*”: “What happens if users know (or believe) that what they are doing is visible to their peers also using the system?” (Lockton et al., 2010, p. 106). Therefore, in designing this task, we remind the broadcaster about “Family”, “Friends”, and “Co-workers” using text that is continually changing and moving (Figure 4.26).



Figure 4.26 The interface of Choosing Your Appearance Directly Task. The photo representing the broadcaster taken from (SiteSell Blog, 2015)

We also used the pattern “*Surveillance*”: “What happens if users know (or believe) their behavior is visible to or monitored by people in positions of power/authority?” (Lockton et al., 2010, p. 108). For this reason we added “Employers” and “Strangers” to the included text (Figure 4.26).

2. *Perceptual Lens*. We used standard and blurred self-portrait live video metaphors.
3. *Interaction Lens*. We used the pattern “Simulation and Feedword”.

### ***Response Stage***

1. From Errorproofing Lens, we used the pattern “*Defaults*”: “Can you make the default setting the behavior you would prefer users to perform?” We made the blurring filter or inpainting (hiding) as the default visual privacy setting for the selected blurred self-portrait, whereas the selected standard self-portrait explicitly shows the broadcaster’s appearance.

### ***User Control***

See Section User Control in 4.2.2.

## **4.3 Design Evaluation Procedure**

In this section we explain how we evaluated our prototypes, outlining the targeted participants, the general procedure of the study, and describing each experiment.

We have proposed design awareness mechanisms in the context of live video broadcasting that address two issues: disclosure of broadcaster location and regrettable broadcasting behavior while intoxicated or negative mental states. We next sought to examine user acceptance of both proposed mechanisms. For the location viewing mechanisms, we were particularly interested in whether the information displayed would be useful and interpreted as intended. For the visual privacy protection mechanisms, we wanted to examine whether the tasks would be understandable and easy to perform for both drunk and non-drunk people.



### **4.3.1 Participants and recruitment**

The target population for the study consisted of users of YouNow, Meerkat, Periscope or other similar apps. We aimed to recruit 18, 24 or 30 participants, as the ideal number of participants was any multiple of 6 due to the experimental setup. Specifically, each participant will be presented with all three prototypes. The order of presentation will be counterbalanced. Because there are 6 possible orders for three prototypes, it is ideal to test a multiple of 6 participants (i.e., 12, 18, 24, 30 etc.), with 1 participant of each set of 6 assigned to each order. Systematic order effects are not anticipated, but such a design can test for them.

We recruited participants from Dalhousie University and the surrounding community who use any live video broadcasting social applications. Specifically, recruitment targeted students, staff and faculty in the Faculty of Computer Science through material posted online (i.e., the faculty list server: see appendix D) and/or on bulletin boards. However, recruitment was not specifically limited to that faculty; if other interested persons saw the recruitment material and wish to participate, they were invited to do so.

The study consisted of two three-phase experiments that were conducted on Dalhousie's campus, in a private room within the Faculty of Computer Science. Both experiments were completed in a single hour session, and each participant received \$20 as compensation. The participants for this portion of the study were different than those that participated in the survey study.

### **4.3.2 Study Procedure**

For each prototype, we described its goal and explained its unique functions. This explanation was kept brief, as pilot sessions prior to the main experiment revealed that providing too detailed a description would lead to boredom among the participants. The study had a within-subjects design. Each session began with a consent form to sign (See Appendix E), and then a short survey to collect basic demographic information (age group, gender, educational group), as well as more detailed information about use of live streaming video applications such as YouNow, Meerkat and Periscope (see Appendix F). Thereafter, the participant completed two three-phase experiments: one experiment evaluated the three prototypes related to location viewers, while the

other evaluated the three prototypes designed for visual privacy protection. In the case of each of the six prototypes, the researcher explained how it works on an iPhone device provided by the researcher. After that, the participant was given the device, so that they could interact freely with the prototypes; the participant was encouraged to think out loud. For each prototype, after familiarization, the participant was given a questionnaire asking about that prototype's design. Details specific to each of the two experiments are discussed below. At the end of the session, the participant was given a final questionnaire to rate the all related designs/prototypes and to comment on their willingness to use or interest in the feature.

### ***Research Hypothesis***

The research hypothesis was that, overall the prototypes (Location Viewers Feedback, and Visual Privacy Awareness prototypes) would receive different ratings. This is because the prototypes have different interfaces. However, the interesting research hypotheses are associated with each task participants were required to complete. For each task, the research hypothesis was that the different prototypes would produce different levels of performance. This prediction is based on the fact that the different prototypes use different techniques to complete the tasks. However, it is difficult to be more precise because these prototypes represent new processes layered on top of a recently developed application and interface.

For each the null hypothesis is that there would be no difference in the level of performance across the prototypes. The alternative to the null is that they would be different (i.e., the alternative to the null is the research hypothesis).

$H_0$ :  $\mu_{\text{GeoLocate}} = \mu_{\text{GeoWatch}} = \mu_{\text{GeoBar}}$  on each measure

$H_0$ :  $\mu_{\text{MMT}} = \mu_{\text{AMT}} = \mu_{\text{ADT}}$  on each measure

### **4.3.3 Location Viewers Feedback Experiment**

To evaluate the proposal prototypes related to location viewing, participants were given a general scenario to imagine while interacting with each prototype:

*In each phase imagine that you are creating a broadcast using this phone (iPhone 6 device is shown to the user). Imagine that the image of the man (an image of a man*

*displayed on the iPhone and shown to the user) represents you as you are broadcasting. The location-showing feature is turned on (for whatever reason).*

Three mechanism designs/prototypes were evaluated to the participants one by one. We counterbalanced the order of presenting them across participants. We tested three prototypes that provide feedback on the identity and location of viewers (see Section 4.1). The three prototypes differ in the manner in which they provide the identity and location of the viewers who checked the broadcaster's location. For each prototype, the participant was asked to interact with the prototype and try to understand the functionality deeply. After the participant interacted with each prototype, he or she was asked in a questionnaire to identify the number of viewers, and the specific identities or locations (or distances) for various individuals (i.e., closest, furthest, moving toward, moving away, location of Person X, location of Person Y) (see Appendix G). The purpose of these questions was to examine the participant's understandability. The time required to do the questionnaire was measured, as was accuracy (number of correct answers). Participants then rated that prototype on functionality, ease of use, and layout (aesthetics). Some questions were adopted and modified from other studies (e.g., Question 14 (d, f, m) from (Lillebo, 2011) and Question 14 (i) from (Zhou, 2015)) (see Appendix G). After viewing all three prototypes, the participant ranked the three and commented on their "willingness to use" or "interest in" the app (see Appendix G). The analysis will examine ratings as a function of prototype.

#### **4.3.4 Visual Privacy Awareness Experiment**

To evaluate the three prototypes, participants were given a general scenario to imagine while interacting with the prototypes:

*In each phase imagine that you are creating a broadcast using this phone (iPhone 6 device is shown to the user). When you turn on the app to start your broadcast, you will see a screen like this (an interface of the task is shown to the participant). Based on your responses and choices, the app will set appropriate default setting for privacy. The app will blur or hide your face or appearance depending on your actions.*

After interacting with each prototype, the participant rated that prototype on functionality, ease of use, and layout (aesthetics), as shown in Appendix H. There is question adopted and modified from another study (Q1 (j) from (Lillebo, 2011). After viewing all three prototypes, the participant ranked three prototypes (see Appendix H) and commented on their “willingness to use” or “interest in” the app. Participants also rated their preference for a privacy setting that “blurs” their appearance or for a privacy setting the “hide” their image on the live video entirely, showing a default background (see Appendix H).

## **4.4 Results**

### **4.4.1 Participants Demographic**

There were 16 males and 5 females. Age was coded as 1 (“19-23 years old”), 2 (“24-28 years old”), 3 (“29-33 years old”), 4 (“34-39 years old”), and 5 (“39-43 years old”). Mean age was 2.14 (SD: 0.85) with sample sizes of 3, 14, 3, 0 and 1 respectively. This is in the 24 -28 range Educational level (highest degree *completed*) was coded a 1 (“Less than High School”), 2 (“High school graduate (includes equivalency)”), 3 (“College or Trade School”), 4 (“Undergraduate Degree”) and 5 (“Graduate Degree, Post-graduate Degree (e.g. DLL), or Professional Degree (e.g., Law, Architecture)”). The mean was 4.43 (SD: 0.93), with samples of 0, 1, 2, 6, 11, and 1. Note that most had graduate degrees. Mean self-reported comfort with technology (coded from 0 “very comfortable” to 6 “very uncomfortable”) was 2.43 (SD: 1.88), ranging from 1 to 6. Mean self-reported knowledge of security (coded as 0 “I have no knowledge at all”, 1 “I have minimal knowledge”, 2 “Good: I feel secure”, and 3 “Expert: I provide advice and assistance”) was 2.29 (SD: 0.56) and ranged from 1 to 3. All participants currently resided in the Halifax region, and most were associated with Dalhousie University.

#### 4.4.2 Self-Reported Behavior of Participants

##### *Live Video Broadcasting App Use*

Use of Periscope YouNow, Meerkat and Periscope or “other apps” was coded on a seven-point scale as “Never” (0), “Less than once a month” (1), “Once a month” (2), “Once a week” (3), “Several times a week” (4), “Once a day” (5), and “Several times a day” (6). The number of users and the amount of use (Frequency) are provided in Table 4.1. Note that the use of Periscope is the highest in terms of number of users (28) and in terms of the amount of use. A mean of 2.02 corresponds to use that is between “Once a month” and “Once a week”.

Table 4.1 Use of Apps

App	Any Use	Exclusive Use		Frequency (Intensity of Use)			
		<i>N</i>	%	Mean	SD	Min	Max
Periscope	17	11	64.7	2.42	1.87	0	6
YouNow	6	1	16.7	0.94	1.65	0	6
Meerkat	6	1	16.7	0.83	1.67	0	6
Other	3	0	0.0	1.60	1.67	0	4

Respondents were asked “Why did you start (or join) a live streaming video app? (select all that apply)” with a subsequent yes/no checklist. Table 4.2 presents the percent endorsement of the items pertaining to use the reasons for use. In addition to the cited reasons, seven included “other” reasons: “share fun things” (coded as entertainment), “To watch other live events” (coded as entertainment), “monitoring the specific audience (coded as professional), to look at different lives in other countries (coded as entertainment), “to view live events or sport (coded as entertainment), “family and friends” (coded as offline friends), and “to benefit from other broadcasters, ideas and for tourism purpose (food, shopping)” (coded as business) The final degrees of endorsement are presented in Table 4.2.

Table 4.2 Reasons for Using Live Streaming Video Apps.

	Option	Endorsement %
1	to maintain contact with friends I know online	38.1
2	to maintain contact with friends I know offline	38.1
3	to maintain contact with strangers online	23.8
4	to find new friends online	33.3
5	to find new followers/fans online	33.3
6	to advocate for change	4.8
7	to help people in need (e.g. who suffer from depression)	0.0
8	to advise young people	14.3
9	to promote my professional profile	33.3
10	to promote my business or activities that I am involved in	33.3
11	to promote my events or event that I am involved in	42.9
12	for entertainment	23.8

It seems that participants used broadcasting mostly for promoting events (42.9%), and for maintaining relationships (38.1%), but not for advising/advocating of helping. When promoting events, it would be expected that users would reveal their location because this would be the location of the promoted event (in rare cases, this might not be true). However, for the other uses, revealing one's location would not necessarily be the default choice.

Participants were asked about the nature of their broadcasts using a simple yes/no checklist format. Data was collected within five categories: Formal broadcasts of Self, Informal broadcasts of Self, Formal broadcasts of Others, Informal broadcasts of Others and Other (non-human) broadcasts, For each category data was collected within three levels of audience (Private to a Single Person, Private to Multiple Persons, and Public), within two levels of planning (Planned and Spontaneous), and within five levels of location (Work, Home, Public, Parties, and while Driving).

Table 4.3 presents the type of audience. The Any column is the total number of participants within each Category of broadcast. For example, 15 of the 21 participants (71.4%)

engaged in Formal broadcast of Self. The Private-Single column is the number who endorsed Private broadcasts to a single individual. The cited percentage is the percent of those making that type of broadcast. For example, 2 participants engaged in Formal broadcasts of Self to a Private-Single audience. In other words, 13.3% of the total number of participants made that type of broadcast.

Table 4.3 Categories of Broadcasts and the Types of Audience for Each Category.

Category of broadcast	Any		Private				Public	
			Single		Multiple			
	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%	<i>N</i>	%
Formal broadcasts of Self	15	71.4	2	13.3	10	66.7	3	20.0
Informal broadcasts of Self	21	100.0	2	9.5	12	57.1	6	28.6
Formal broadcasts of Others	17	81.0	2	11.8	4	23.5	8	47.1
Informal broadcasts of Others	17	81.0	2	11.8	8	47.1	3	17.6
Non-Human broadcasts	18	85.7	1	5.6	1	5.6	15	83.3
Any Category	21	100.0	5	23.8	19	90.5	17	81.0

Notes: Total sample size is 21.

Note that all participants engaged in Informal broadcast of Self. Within each Category, most were Private-Multiple, with the exception of Non-Human broadcasts. Across Categories (the Any Category row), Private-Multiple was only slightly higher than Public. Note that Informal broadcast created the possibility of higher self-disclosure but the privacy and security issues are lower because most are private. Table 4.3 implies that participants do care about their privacy because they use private broadcasts more often than public broadcast. This is likely due, in part, to the fact that most participants used Periscope, which is the only app that provides this ability to narrowcast.

In addition, most participants (95.2% of 21) engaged in a mix of broadcast Categories (2 or more of the 5) and 57.1% engaged in all five Categories. The mean number of Categories was 4.19 (SD 1.17).

There was a slight tendency for more broadcast of Self (formal or informal). That is, participants who endorsed either Formal broadcast of Self or/and Informal broadcast of Self were coded as broadcast of Self. Broadcast of Self were endorsed by 100.0% of respondents while broadcast of Others (formal or informal) were endorsed by 90.52%. Broadcasts of self may have fewer issues of privacy because the broadcast is not likely to capture other individuals (without consent).

Formal broadcasts (self or other) and Informal broadcast (self or other) were endorsed at the same rate (90.5%). Table 4.4 presents the correlations between any broadcast use within Categories.

Table 4.4 Correlations between Categories of Broadcasts (BCs)

	Formal BCs of Self	Informal BCs of Self	Formal BCs of Others	Informal BCs of Others	Non-Human BCs
Formal BCs of Self	1.000	NA	0.230	0.230	0.043
Informal BCs of Self		1.000	NA	NA	NA
Formal BCs of Others			1.000	0.382	<b>0.842</b>
Informal BCs of Others				1.000	<b>0.495</b>
Non-Human BCs					1.000

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 21$  for all comparisons.

These are equivalent to phi-correlations.

NA = the correlation could not be computed because everyone indicated Informal broadcasts of Self.

Note that all are positive, and two are significant ( $p < 0.05$ ). Thus, one can say that most people engage in a multitude of broadcast types.

Table 4.5 provides the degree of planning associated with each type of broadcast (the Any is repeated to provide context). Within each category, respondents could indicate that



broadcasts were planned *and/or* spontaneous (i.e., they could choose both), but no one did (all reported either planned or spontaneous — *within* a Category). All percentages are relative to the number of participants who endorsed the category (e.g., 13 is 88.7% of 15).

Table 4.5 Categories of Broadcasts (BCs) and the Types of Planning for Each Category.

Category of BCs	Any	Planned		Spontaneous	
	<i>N</i>	<i>N</i>	%	<i>N</i>	%
Formal BCs of Self	15	13	86.7	4	26.7
Informal BCs of Self	21	2	9.5	19	90.5
Formal BCs of Others	17	8	47.1	9	52.9
Informal BCs of Others	17	3	17.6	13	76.5
Other BCs (non-human)	18	3	16.7	14	77.8
Any Category	21	17	81.0	20	95.2

Planned broadcasts are more common with the Formal broadcast of Self but not for Formal broadcasts of Others. Spontaneous broadcast were more common with Informal broadcast of Self and this was also true for Informal broadcast of Others.

More generally, if either (or both) Formal broadcast of Self or Formal broadcast of Others were planned, the participant was scored as Formal planned. If either (or both) Informal broadcast of Self or Informal broadcast of Other were planned, the participant was scored as Informal planned. Planning was more common with the Formal broadcasts (endorsed by 71.4%) than with the Informal broadcasts (57.6%). Conversely, spontaneity was more common with Informal broadcasts (95.2%) than with Formal broadcasts (about 57.1%).

Furthermore, across all categories, only 4.3% (1) indicated that *all* broadcasts were planned, whereas 19.0% (4) indicated that *all* broadcasts were spontaneous and 72.6% (16) indicated a mix of planned and spontaneous broadcasts. The correlation between planned and spontaneous (collapsed over Categories) was  $r = -.108$  ( $p < 0.639$ ). That is, the two types were not associated. It seems that all participants do a bit of both.

For those participants who primarily use broadcasting for promoting events, Formal

Planned broadcasts would be expected, and privacy issues would be minimal (i.e., the point is publicity). On the other hand, those that use broadcasts for maintaining relationships (likely informal and spontaneous) might have more privacy issues depending on the viewers (online strangers would be more of an issue than offline friends).

Table 4.6 provides the location of broadcasts, again within each category (the Any is repeated to provide context). All values are expressed as the proportion of individuals within each broadcast type (i.e., 44.8% of the 24 users who created Formal broadcast of Self did so at work).

Table 4.6 Categories of Broadcasts (BCs) and the Locations of those Broadcasts.

Category of broadcast	Any			Work		Home		Public		Parties		Stims		Driving	
	N	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Formal BCs of Self	15	14	93.3	9	60.0	4	26.7	0	0.0	0	0.0	0	0.0	0	0.0
Informal BCs of Self	21	4	19.0	14	66.7	10	47.6	9	42.9	2	9.5	3	14.3		
Formal BCs of Others	17	11	64.7	3	17.6	9	52.9	1	5.9	0	0.0	1	5.9		
Informal BCs of Others	17	2	11.8	6	35.3	12	70.6	4	23.5	1	5.9	0	0.0		
Non-Human broadcasts	18	0	0.0	5	27.8	12	66.7	3	16.7	0	0.0	2	11.1		
Any Category	21	18	85.7	19	90.5	19	90.5	12	57.1	2	9.5	4	19.0		

Firstly, most broadcasts are conducted at home (endorsed by 90.5% of participants) or in public places (endorsed by 90.5%). However, broadcasts at work (85.7%) are almost as high. broadcasts at parties (about 57.1%) are lower. Note that broadcasts while driving are relatively low (endorsed by only 19.0% of respondents). Broadcasts while under the influence of stimulants (e.g., alcohol, recreational drug) are the lowest (9.5%).

There were five different locations. Collapsed over Categories of broadcast, respondents indicated the use of an average of 3.43 (SD: 1.12) different locations (range 1 to 5). This count did not include Stimulants because that is not truly a location. Within each Category, the numbers were smaller with a means of 1.29 (SD: 0.90) for Formal broadcasts of Self, 1.90 (SD: 1.18) for Informal broadcasts of Self, 1.19 (SD: 0.93) for Formal BsC of Others, 1.14 (SD: 1.01) for Informal broadcasts of Others, and 1.05 (SD: 1.12) for Other broadcasts (non-human). This

implies that most respondents only used a single location within each category of broadcast. Table 4.7 presents the correlations between locations collapsed over Categories.

Table 4.7 Correlations between the Locations of Broadcasts.

	Work	Home	Public	Parties	Stimulants	Driving
Work	1.000	-0.132	0.331	0.196	-0.331	0.198
Home		1.000	-0.105	0.047	0.105	0.157
Public			1.000	0.375	<b>-0.447</b>	0.157
Parties				1.000	-0.047	0.420
Stimulants					1.000	-0.157
Driving						1.000

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 44$  for all comparisons.

These are equivalent to phi-correlations.

Note most are *not* significant ( $p > 0.05$ ) and near zero. As such, it seems that across categories, participants do not use the same locations consistently. That is, the respondents who use the home Informal broadcast of Self are not *necessarily* the same respondents who use the home for Formal broadcasts of Self. Simply, there is little consistency.

Participants were asked, “In broadcasts, would you like to keep the following sensitive information private (choose all that apply)?” Responses were collected using a six-point (0 “strongly disagree” to 5 “strongly agree”). The options (simplified) are presented in Table 4.8. For the open-ended responses, five participants wrote “A visual of anything that can help strangers identify me, e.g.- my university id card”, “Personal information such as name, job, etc.”, “I will always want to keep my information private especially if its personal or issues that are 'domestic'.” “Vehicle number plates, Home address” and “My name. User name is not my true name”

Table 4.8 Endorsement of Options about Sensitive Information (to be Kept Private)

		Mean	SD	Min	Max
1	my face	2.71	1.35	1	5
2	my voice	2.24	1.30	1	5
3	my exact GPS location	4.19	0.98	2	5
4	my approximate location	3.38	1.12	2	5
5	the visual of my surroundings	2.65	1.31	1	5
6	the people in my surroundings	3.50	1.36	1	5
7	my inappropriate behavior	4.35	1.04	1	5
8	the inappropriate behavior of others	3.95	1.32	1	5

Note that the only option with high endorsement is location. The second highest is inappropriate behavior, though that might be difficult to achieve with current technology (and requires a definition of “inappropriate”). It seems that users are concerned about these two types of information: location, and the inappropriate behavior. These are linked to the purpose of the current study.

Finally, participants were asked “People should be careful about their moods while broadcasting because (check all that apply):”, with options that included “a person could make inappropriate comments while in negative moods”, “a person could engage in inappropriate or illegal actions while in negative moods”, “employers could be watching which could create a negative opinion of the broadcaster”, “friends could be watching which could create a negative opinion of the broadcaster” and “strangers could be watching which could create a negative opinion of the broadcaster” The percent endorsement of each is provided in Table 4.9.

Table 4.9 Endorsement of Options about Moods.

	<i>N</i>	<i>%</i>
Care about Moods: Comments	18	85.7
Care about Moods: Actions	15	71.4
Care about Moods: Employer	18	85.7
Care about Moods: Strangers	14	66.7
Care about Moods: Friends	14	66.7

All the percentages are above 60 and comparable. This implies that participants agree that the negative mood causes negative consequences while broadcasting. Hence, it is important to have “checks” on mood.

#### 4.4.3 Comparison of Prototypes

##### 4.4.3.1 Location Viewers Feedback Prototypes (GeoLocate, GeoWatch, GeoBar)

###### *Number of Viewers*

Participants were asked to count the number of viewers who had examined the broadcaster’s location (Count of Viewers: Question 1). The correct value was 8 for all prototypes. Table 4.10 provides the descriptive statistics.

###### 4.10 Number of Viewers Identified Correctly (out of 8)

Prototype	Eight Correct		Statistics				
	Num	<i>%</i>	Min	Max	NA	Mean	SD
GeoLocate	20	95.2	8	8	1	8.00	0.00
GeoWatch	12	57.1	5	8	0	7.32	0.95
GeoBar	12	57.1	3	8	1	6.89	1.52

Notes: NA = No Answer

The *Eight Correct* is the number of participants who obtained the correct value (8). The *Statistics* is the “range” of responses. For example, for GeoWatch and GeoBar, the minimum are 5 and 3 implying that some participants could not count the viewers successfully. Using a one-way within-subjects ANOVA with three levels of Prototype, the means for *Eight Correct* were significantly different with  $F(2,40) = 5.298$  ( $p < 0.010$ ,  $\eta^2 = 0.227$ ). Follow-up planned within-subjects *t*-tests (also called paired *t*-tests or repeated measures *t*-tests) showed that GeoLocate was higher than GeoWatch ( $t(40) = 3.152$ ,  $p < 0.006$ ) and that GeoLocate was higher than GeoBar ( $t(40) = 3.157$ ,  $p < 0.005$ ), but that GeoWatch and GeoBar did not differ ( $t(40) = 0.984$ ,  $p < 0.338$ ).

The correlations across participants, between the *Eight Correct* were computed. However, because all scores for GeoLocate were 8 (with one missing value), the correlations between GeoLocate and GeoWatch and between GeoLocate and GeoBar could not be computed. The correlation between GeoWatch and GeoBar was  $r = -.146$  ( $p < 0.568$ ). The negative correlation is not significant meaning that it is effectively zero and there is no association. That is, the participants with the highest performance on GeoWatch may have been the best, worst or in the middle on GeoBar (and vice versa).

GeoLocate was superior for the identification of the number of viewers as above in the analysis.

### *Viewer Identification*

Participants were asked to list the actual viewers who had examined the broadcaster’s location (Question 2). On the prototypes, viewers were identified generically as Man 1, Man 2, through Man 9 and Lady 1, Lady 2, through Lady 9. There were 8 (of a potential 18) to be identified. A correct response involved the proper identification of all 8, and only the proper 8. Responses that were similar to “8 viewers” or “anyone who using application” were considered incorrect. In Table 4.11, *Correct ID: 8 Viewers* is the number of participants who properly identified all 8. As can be seen in Table 4.11, most participants did not identify all 8, but GeoLocate was much higher than the other 2 prototypes. For GeoLocate, 13 participants correctly identified all 8, whereas for GeoWatch and GeoBar, the numbers were much lower at 4 and 2 respectively. Table

2 provides the correct responses, as well as two types of errors (Exclusions and Intrusions).

Table 4.11 Number of Participants who Correctly Identified (cited) the Individual Viewers (out of 8)

Prototype	Correct ID 8 Viewers		Exclusions				Intrusions			
	Num	Percent	Mean	SD	Min	Max	Mean	SD	Min	Max
GeoLocate	13	61.9	2.19	3.30	1	8	0.10	0.30	0	1
GeoWatch	4	19.0	3.38	3.34	1	8	0.19	0.51	0	2
GeoBar	2	9.5	3.43	2.86	1	8	0.10	0.30	0	1

For *Correct ID: 8 Viewers*, a one-way within-subjects ANOVA with three levels of Prototype showed that the mean performance differed with  $F(2,40) = 10.785$  ( $p < 0.0005$ ,  $\eta^2 = 0.350$ ). Follow-up planned within-subjects  $t$ -tests (also called paired  $t$ -tests or repeated measures  $t$ -tests) showed that GeoLocate was higher than GeoWatch ( $t(40) = 3.300$ ,  $p < 0.005$ ) and that GeoLocate was higher than GeoBar ( $t(40) = 4.000$ ,  $p < 0.001$ ), but that GeoWatch and GeoBar did not differ ( $t(40) = 1.000$ ,  $p < 0.329$ ).

An Exclusion Error was a failure to identify some of the 8 viewers. Exclusion Errors ranged from 0 (i.e., those who correctly identified all 8) to 8 (i.e., those who got none of the 8). A similar one-way within-subjects ANOVA (three levels of Prototype) showed that the mean performance on Exclusion Errors did *not* differ with  $F(2,40) = 1.944$  ( $p < 0.156$ ,  $\eta^2 = 0.089$ ). Follow-up planned within-subjects  $t$ -tests showed that GeoLocate and GeoWatch did not differ ( $t(40) = 1.508$ ,  $p < 0.147$ ), that GeoLocate and GeoBar did not differ ( $t(40) = 1.666$ ,  $p < 0.111$ ), and that GeoWatch and GeoBar did not differ ( $t(40) = 0.082$ ,  $p < 0.936$ ).

Intrusion Errors refer to the citing of a viewer who did *not* exist. Intrusion errors ranged from 0 (no intrusions) to 2. A one-way within-subjects ANOVA (three levels of Prototype) showed that the mean performance on Intrusion Errors did *not* differ with  $F(2,40) = 0.559$  ( $p < 0.576$ ,  $\eta^2 = 0.027$ ). Follow-up planned within-subjects  $t$ -tests showed that GeoLocate and GeoWatch did not differ ( $t(40) = 0.805$ ,  $p < 0.428$ ), that GeoLocate and GeoBar did not differ ( $t(40) = 0.000$ ,  $p < 1.000$ ), and that GeoWatch and GeoBar did not differ ( $t(40) = 1.000$ ,  $p < 0.329$ ).

As noted above viewers on the prototypes were identified as Man 1, Man 2, through Man

9 and Lady 1, Lady 2, through Lady 9. Hence, an Exclusion or Intrusion Error could be a mistake of typing numbers. This is a fairly stringent test of usability because the “names” are quite confusable, and likely more so than would in general operation.

The correlations for *Correct ID: 8 Viewers* across participants were computed. For GeoLocate and GeoWatch,  $r = 0.131$  ( $p < 0.571$ ), for GeoLocate and GeoBar,  $r = -0.080$  ( $p < 0.732$ ) and for GeoWatch and GeoBar,  $r = 0.256$  ( $p < 0.256$ ).

With respect to the identification of particular viewers, GeoLocate was clearly superior. The other two prototypes were equivalent. However, all three prototype are about the same on Exclusion and Intrusion Errors GeoLocate was superior because participants identified all 8 — and only 8 — viewers.

### *Viewer Distance*

For the general identification of the location (city) of the viewers, we asked, “Which country/city they are belong to? "If the app cannot do this, please skip"”. The number of correct answers for GeoLocate was 16 (76.2%), for GeoWatch was 15 (71.4) and for GeoBar was 15 (71.4%). Using a one-way within-subjects ANOVA with three levels of Prototype, the difference was not significant with  $F(2,40) = 0.16$  ( $p < 0.853$ ,  $\eta^2 = 0.008$ ). Thus, the operation was equally easy on all prototypes.

Participants were asked to record the distances to each individual viewer (Question 4). There were 8 distances to be identified. For this analysis, only the proper 8 viewers were considered (i.e., a distance associated with an Exclusion or Intrusion error was not considered). Most viewers were static so there was one correct value. Some viewers were in motion, so there was range of possible acceptable values. Responses that were similar to “within Halifax”, “NEAR ME” or “within my city” were considered incorrect (a missing response). Responses that included a numerical value like “15–60km away” or “Up to 45km away” were coded as a single value (at the midpoint for the range if there was a range), and then coded in the manner of a correct response. As can be seen in Table 4.12, performance was not high (but highest in GeoLocate), but one must note that the previous failure to identify the correct viewers likely carries over to the identification of distances. That is, of the 13 participants who correctly identified all the viewers in GeoLocate (see Table 4.11), only 9 correctly identified all the



distances. One additional participant had a single error reporting a distance of 32 as 22 and another reported a distance of 40 as 4 (likely typos). For GeoWatch, the errors were more general. Only 8 participants identified distances, and of the 8, 5 missed one or more viewers. There were no transcription errors (typos). For GeoBar, 10 participants identified distances, but 9 of those 10 missed some viewers (1 participant missed 1 viewer, and 8 participants missed 2 viewers) and/or transcribed in appropriate distances (e.g., one participant recorded distances of 6 to 13.5, 5, and 6.5 to 14 all as “at my location” which was coded as a distance of 0).

Table 4.12 Number of Participants who Correctly Identified the Distance to each (cited) Viewer (out of 8)

Prototype	Correct Distances	
	Num	%
GeoLocate	9	42.9
GeoWatch	3	14.3
GeoBar	1	4.8

A one-way within-subjects ANOVA (three levels of Prototype) showed that the mean number of *Correct Distances* differed with  $F(2,40) = 6.582$  ( $p < 0.003$ ,  $\eta^2 = 0.248$ ). Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch differed ( $t(40) = 2.344$ ,  $p < 0.030$ ), that GeoLocate and GeoBar differed ( $t(40) = 2.953$ ,  $p < 0.008$ ), but that GeoWatch and GeoBar did not differ ( $t(40) = 1.439$ ,  $p < 0.162$ ).

The correlations for *Correct Distances* across participants were computed. For GeoLocate and GeoWatch,  $r = 0.196$  ( $p < 0.393$ ), for GeoLocate and GeoBar,  $r = -0.194$  ( $p < 0.400$ ) and for GeoWatch and GeoBar,  $r = 0.548$  ( $p < 0.010$ ). The fact that the first two are not significant implies the participants with the highest performance on GeoLocate were not necessarily the highest on GeoWatch or GeoBar (i.e., they could have been the highest, the lowest, or in the middle). However, the fact that the last correlation is significant (and “moderate”) implies that those with the highest scores on GeoWatch also had the highest scores on GeoBar. That is, for this task GeoWatch and GeoBar seem to tap some common skills which could be “attention to detail” or “visual acuity”.

With respect to the distance to particular viewers, GeoLocate was clearly superior.

### *Viewers Appearing*

Participants were asked to note who “suddenly appeared” (Question 5). For GeoLocate, this was not possible to determine, so the correct answer is none or unable to determine. Note that ““If the app cannot do this, please skip”” was a response option. Hence, citing “not doable”, “zero” or “none” as a valid option. For GeoWatch and GeoBar, the correct number was 2. Participants were scored for identifying the correct number. Table 4.13 includes the Correct Responses, and the Exclusion and Intrusion Errors.

Table 4.13 Number of Participants who Correctly Identified the Individual Viewers who Suddenly Appeared Onscreen (out of 2)

Prototype	Correct ID Appeared		Exclusions: Appeared				Intrusions: Appeared			
	Num	%	Mean	SD	Min	Max	Mean	SD	Min	Max
GeoLocate	12	57.1	na	na	na	na	0.71	0.90	0	2
GeoWatch	13	61.9	1.86	0.36	0	2	0.33	1.11	0	5
GeoBar	12	57.1	1.90	0.30	0	2	0.52	1.36	0	6

Notes: na is not applicable

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Correct ID Appeared* did not differ with  $F(2,40) = 0.087$  ( $p < 0.917$ ,  $\eta^2 = 0.004$ ). Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were the same ( $t(40) = 0.329$ ,  $p < 0.748$ ), that GeoLocate and GeoBar were the same ( $t(40) = 0.000$ ,  $p < 1.000$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 0.372$ ,  $p < 0.715$ ).

As above, Exclusion and Intrusion Errors were noted, but Exclusion Errors were not possible with GeoLocate (because the correct response did not include any viewers so it was not possible to exclude any). Exclusion Errors ranged from 0 (i.e., those who correctly both) to 2 (i.e., those who identified neither of the 2). The mean number of exclusions was above 1 for all prototypes, consistent with the lower overall performance (i.e., only 50 - 60% of participants were correct). A one-way within-subjects ANOVA (2 levels of Prototype — GeoLocate did not

apply) showed that the mean performance for *Exclusions: Appeared* did not differ with  $F(1,20) = 0.192$  ( $p < 0.666$ ,  $\eta^2 = 0.010$ ).

Intrusion Errors could range from 0 to 16 (there were 18 possible viewers, but 2 represented the proper response) but actually ranged from 1 to 6 (that is, participants only listed up to 6 viewers that they “believed” had suddenly appeared. The mean number of intrusions was 0.7 for GeoLocate (recall that all errors would be intrusions) and about 0.3 for GeoWatch and about 0.5 for GeoBar. A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Exclusions: Appeared* did not differ with  $F(2,40) = 0.836$  ( $p < 0.441$ ,  $\eta^2 = 0.004$ ). Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were the same ( $t(40) = 1.165$ ,  $p < 0.258$ ), that GeoLocate and GeoBar were the same ( $t(40) = 0.505$ ,  $p < 0.618$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 1.696$ ,  $p < 0.104$ ).

The correlations for *Correct ID: Appeared* across participants were computed. For GeoLocate and GeoWatch,  $r = 0.113$  ( $p < 0.625$ ), for GeoLocate and GeoBar,  $r = 0.417$  ( $p < 0.060$ ) and for GeoWatch and GeoBar,  $r = 0.311$  ( $p < 0.169$ ). The fact that none are significant implies the participants with the highest performance on GeoLocate were not necessarily the highest on GeoWatch or GeoBar (i.e., they could have been the highest, the lowest, or in the middle), and those with the highest on GeoWatch were not necessarily the highest on GeoBar. On the one hand, the lack of significance implies that the different prototypes tap different skills. On the other hand, the lack of significance is an issue of the low sample size (just 21) and all of the correlations are positive and of reasonable size (“moderate” in the range 0.316 to 0.707). Hence, it is likely that successful use of the three prototypes requires some common skill. The most likely candidates are “attention” (“focus”) or “visual acuity”.

For finding the identities of those who appeared, users of every prototype, except GeoLocate, were equivalently successful at identifying viewers whose identities were revealed. Users of the GeoLocate prototype correctly noted that the prototype did not allow them to identify their viewers.

### *Disappearing Viewers*

Participants were asked to note who “suddenly disappeared” (Question 6). For GeoLocate, this was not possible to determine, so the correct answer is none or unable to determine. Note that

““If the app cannot do this, please skip”” was a response option. Hence, citing “not doable”, “zero” or “none” as a valid option. For GeoWatch and GeoBar, the correct number was 2. Participants were scored for identifying the correct number. Table 4.14 includes the Correct Responses, and the Exclusion and Intrusion Errors.

Table 4.14 Number of Participants who Correctly Identified the Individual Viewers who Suddenly Disappeared Onscreen (out of 2)

Prototype	Correct ID Disappeared		Exclusions: Disappeared				Intrusions: Disappeared			
	Num	Percent	Mean	SD	Min	Max	Mean	SD	Min	Max
GeoLocate	17	81.0	na	na	na	na	0.43	1.33	0	6
GeoWatch	10	47.6	0.90	0.94	0	2	0.19	0.40	0	1
GeoBar	12	57.1	0.71	0.90	0	2	0.14	0.36	0	1

Notes: na is not applicable

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Correct ID Disappeared* differed with  $F(2,40) = 4.561$  ( $p < 0.016$ ,  $\eta^2 = 0.186$ ). Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were different ( $t(40) = 3.171$ ,  $p < 0.005$ ), but that GeoLocate and GeoBar were the same ( $t(40) = 2.017$ ,  $p < 0.056$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 0.805$ ,  $p < 0.428$ ).

As above, Exclusion and Intrusion Errors were noted, but Exclusion Errors were not possible with GeoLocate (because the correct response did not include any viewers so it was not possible to exclude any). Exclusion Errors ranged from 0 (i.e., those who correctly both) to 2 (i.e., those who identified neither of the 2). The mean number of exclusions was about 1 for both GeoWatch and GeoBar. A one-way within-subjects ANOVA (2 levels of Prototype — GeoLocate did not apply) showed that the mean performance for *Exclusions: Disappeared* did not differ with  $F(1,20) = 0.884$  ( $p < 0.358$ ,  $\eta^2 = 0.042$ ).

Intrusion Errors could range from 0 to 16 (there were 18 possible viewers, but 2 represented the proper response) but actually ranged from 1 to 6. The mean number of intrusions was only 0.4 for GeoLocate (recall that all errors would be intrusions) and about 0.2 for GeoWatch and GeoBar. A one-way within-subjects ANOVA (3 levels of Prototype) showed that

the mean performance for *Exclusions: Disappeared* did not differ with  $F(2,40) = 0.7666$  ( $p < 0.471$ ,  $\eta^2 = 0.037$ ). Follow-up planned within-subjects  $t$ -tests showed that GeoLocate and GeoWatch were the same ( $t(40) = 0.793$ ,  $p < 0.437$ ), that GeoLocate and GeoBar were the same ( $t(40) = 0.973$ ,  $p < 0.343$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 0.571$ ,  $p < 0.576$ ).

The correlations for *Correct ID Disappeared* across participants were computed. For GeoLocate and GeoWatch,  $r = 0.462$  ( $p < 0.035$ ), for GeoLocate and GeoBar,  $r = 0.315$  ( $p < 0.164$ ) and for GeoWatch and GeoBar,  $r = 0.440$  ( $p < 0.046$ ). Note that two of the three were significant and that the third was almost of the same magnitude. All were moderate. Thus, all prototypes seem to tap some common skill for this task. The most likely skills would be “attention” and/or “memory” and/or “visual acuity”. To use all prototype, one must pay attention, remember which viewers were showing, and be able to read the fine print.

For finding the identities of those who disappeared, GeoLocate was superior in the sense that participants correctly noted that they could not perform the task. The performance with the two prototypes that could do the task was the same.

#### *Closest Viewer*

Participants were asked who was the closest (Question 7). There was only one correct response per prototype. Table 4.15 presents the results for the numbers correct, the Exclusions and the Intrusions. Note that because there is only one correct response, the Exclusions is the opposite of the Correct response (i.e., if they did not indicate the one correct answer, they automatically excluded the one correct answer). However, there could be more than one Intrusion (if participants felt that two or more viewers were “closest”).

Table 4.15 Number of Participants who Correctly Identified the Closest Viewer

Prototype	Correct ID Closest		Exclusions: Closest				Intrusions: Closest			
	Num	%	Mean	SD	Min	Max	Mean	SD	Min	Max
GeoLocate	15	71.4	0.29	0.46	0	1	0.38	0.50	0	1
GeoWatch	18	85.7	0.14	0.36	0	1	0.19	0.68	0	3
GeoBar	17	81.0	0.19	0.40	0	1	0.43	0.81	0	2

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Correct ID: Closest* did not differ with  $F(2,40) = 0.870$  ( $p < 0.427$ ,  $\eta^2 = 0.042$ ). Follow-up planned within-subjects  $t$ -tests showed that GeoLocate and GeoWatch were the same ( $t(40) = 1.144$ ,  $p < 0.267$ ), that GeoLocate and GeoBar were the same ( $t(40) = 0.805$ ,  $p < 0.428$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 0.571$ ,  $p < 0.576$ ).

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Intrusions: Closest* did not differ with  $F(2,40) = 1.333$  ( $p < 0.275$ ,  $\eta^2 = 0.062$ ). Follow-up planned within-subjects  $t$ -tests showed that GeoLocate and GeoWatch were the same ( $t(40) = 1.284$ ,  $p < 0.214$ ), that GeoLocate and GeoBar were the same ( $t(40) = 0.298$ ,  $p < 0.771$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 0.1556$ ,  $p < 0.135$ ).

The correlations for *Correct ID: Closest* across participants were computed. For GeoLocate and GeoWatch,  $r = 0.043$  ( $p < 0.853$ ), for GeoLocate and GeoBar,  $r = 0.230$  ( $p < 0.316$ ) and for GeoWatch and GeoBar,  $r = 0.495$  ( $p < 0.022$ ). The fact that the first two are not significant implies the participants with the highest performance on GeoLocate were not necessarily the highest on GeoWatch or GeoBar (i.e., they could have been the highest, the lowest, or in the middle). However, GeoWatch and GeoBar are moderately correlated which implies that these two prototype tap some common skill or cognitive ability. The most likely candidate would be “visual acuity” but it could be “attention to detail”.

For finding the closest viewer, the three prototypes were statistically equivalent.

*Furthest Viewer*

Participants were asked who was the furthest (Question 8). There was only one correct response per prototype. Table 4.16 presents the results for the number correct, the Exclusions and the Intrusions. Note that because there is only one correct response, the Exclusions is the opposite of the Correct response (i.e., if they did not indicate the one correct answer, they automatically excluded the one correct answer). However, there could be more than one Intrusion (if participants felt that two or more viewers were “furthest”).

Table 4.16 Number of Participants who Correctly Identified the Furthest Viewer

Prototype	Correct ID Furthest		Exclusions: Furthest				Intrusions: Furthest			
	Num	%	Mean	SD	Min	Max	Mean	SD	Min	Max
GeoLocate	18	85.7	0.14	0.36	0	1	0.05	0.22	0	1
GeoWatch	18	85.7	0.14	0.36	0	1	0.10	0.30	0	1
GeoBar	18	85.7	0.14	0.36	0	1	0.14	0.36	0	1

Note that the mean number correct on *Correct ID: Furthest*, and mean number of errors (*Exclusion Furthest*) were the same for all prototypes. As such, an ANOVA serves no purpose (i.e.,  $F(2,40) = 0.000, p < 1.000, \eta^2 = 0.000$ ), and all follow-up planned within-subjects *t*-tests are non-significant and identical ( $t(40) = 0.000, p < 1.000$ ).

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Intrusions: Furthest* did not differ with  $F(2,40) = 1.333 (p < 0.275, \eta^2 = 0.062)$ . Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were the same ( $t(40) = 0.571, p < 0.575$ ), that GeoLocate and GeoBar were the same ( $t(40) = 1.000, p < 0.329$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 1.000, p < 0.329$ ).

The correlation for *Correct ID: Furthest* across participants were computed. For GeoLocate and GeoWatch,  $r = 0.611 (p < 0.003)$ , for GeoLocate and GeoBar,  $r = 0.611 (p < 0.003)$  and for GeoWatch and GeoBar,  $r = 0.611 (p < 0.003)$ . All the correlations are the same because the Correct: Furthest have the same counts (totals) and because the correlations are actually phi-coefficients ( $\Phi$ ). In fact, the different prototypes did have different participants who

were successful. The fact that all are significant implies that the prototype all tap some common skill such as “visual acuity” or “attention to detail”.

For finding the furthest viewer, the three prototypes were statistically equivalent.

*Viewers Moving Toward Broadcaster*

Participants were asked who was moving toward the broadcaster’s location (Question 9). There were two correct responses per prototype. Table 4.17 presents the results for the number correct, the Exclusions and the Intrusions. Each participant identified all those that they thought were moving towards the broadcaster. As such, the citations could include the correct two, miss one of both of the correct two (Exclusion Error) or include addition viewers who were not moving (Intrusion Errors).

Table 4.17 Number of Participants who Correctly Identified the Viewers Moving Toward the Broadcaster

Prototype	Correct ID: Toward		Exclusions: Toward				Intrusions: Toward			
	Num	Percent	Mean	SD	Min	Max	Mean	SD	Min	Max
GeoLocate	15	71.4	0.52	0.87	0	2	0.00	0.00	0	0
GeoWatch	15	71.4	0.48	0.81	0	2	0.52	0.75	0	3
GeoBar	12	57.1	0.67	0.86	0	2	0.05	0.22	0	1

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Correct ID: Towards* did not differ with  $F(2,40) = 0.896$  ( $p < 0.416$ ,  $\eta^2 = 0.043$ ). Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were the same ( $t(40) = 0.000$ ,  $p < 1.000$ ), that GeoLocate and GeoBar were the same ( $t(40) = 1.375$ ,  $p < 0.186$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 1.144$ ,  $p < 0.267$ ).

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Exclusions: Towards* did not differ with  $F(2,40) = 0.488$  ( $p < 0.618$ ,  $\eta^2 = 0.024$ ). Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were the same ( $t(40) = 0.205$ ,  $p < 0.841$ ), that GeoLocate and GeoBar were the same ( $t(40) = 0.899$ ,  $p < 0.379$ ),



and that GeoWatch and GeoBar were the same ( $t(40) = 0.936, p < 0.358$ ).

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Intrusions: Toward* differed with  $F(2,40) = 8.315 (p < 0.001, \eta^2 = 0.294)$ . Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were different ( $t(40) = 3.195, p < 0.004$ ), that GeoLocate and GeoBar were the same ( $t(40) = 1.000, p < 0.329$ ), and that GeoWatch and GeoBar were different ( $t(40) = 2.674, p < 0.014$ ).

The correlation for *Correct ID: Toward* across participants were computed. For GeoLocate and GeoWatch,  $r = 0.067 (p < 0.774)$ , for GeoLocate and GeoBar,  $r = 0.517 (p < 0.016)$  and for GeoWatch and GeoBar,  $r = 0.304 (p < 0.180)$ . GeoLocate and GeoBar share or tap a common skill or cognitive ability.

For finding the viewers who are moving toward the broadcaster, all prototypes were about the same, though GeoLocate had slightly lower (no) Intrusion Errors.

#### *Viewers Moving Away from Broadcaster*

Participants were asked who was moving away from the broadcaster’s location (Question 10). There was only correct responses per prototype, and GeoLocate did not provide the information (participants could note that the prototype did not provide the information). Table 4.18 presents the results for the numbers correct, the Exclusions and the Intrusions. Note that even though GeoLocate could not perform the task, there is still the chance for Intrusion Errors. Each participant identified all those that they thought were away from the broadcaster.

Table 4.18 Number of Participants who Correctly Identified the Viewers Moving Away from the Broadcaster

Prototype	Correct ID: Away		Exclusions: Away				Intrusions: Away			
	Num	Percent	Mean	SD	Min	Max	Mean	SD	Min	Max
GeoLocate	19	90.5	na	na	na	na	0.10	0.30	0	1
GeoWatch	11	52.4	0.48	0.51	0	1	0.52	0.75	0	3
GeoBar	14	66.7	0.33	0.48	0	1	0.10	0.30	0	1

Notes: na is not applicable

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Correct: Away* differed significantly with  $F(2,40) = 5.385$  ( $p < 0.008$ ,  $\eta^2 = 0.212$ ). Follow-up planned within-subjects  $t$ -tests showed that GeoLocate and GeoWatch were different ( $t(40) = 3.495$ ,  $p < 0.002$ ), but that GeoLocate and GeoBar were not different ( $t(40) = 2.017$ ,  $p < 0.056$ ), and that GeoWatch and GeoBar were not different ( $t(40) = 1.144$ ,  $p < 0.267$ ). Because there is only one correct response, the Exclusions are the opposite of the Correct, so the analysis is the same.

A one-way within-subjects ANOVA (3 levels of Prototypes) showed that the mean performance for *Intrusions: Away* differed significantly with  $F(2,40) = 5.094$  ( $p < 0.011$ ,  $\eta^2 = 0.203$ ). Follow-up planned within-subjects  $t$ -tests showed that GeoLocate and GeoWatch were different ( $t(40) = 2.424$ ,  $p < 0.025$ ), that GeoWatch and GeoBar were different ( $t(40) = 2.424$ ,  $p < 0.025$ ), but that GeoLocate and GeoBar were the same ( $t(40) = 0.000$ ,  $p < 1.000$ ).

The correlations for *Correct ID: Away* between participants were computed. For GeoLocate and GeoWatch,  $r = 0.340$  ( $p < 0.131$ ), for GeoLocate and GeoBar,  $r = 0.115$  ( $p < 0.621$ ) and for GeoWatch and GeoBar,  $r = 0.337$  ( $p < 0.135$ ). Prototype 1, 2 and 3 do not seem to tap a common skill or cognitive ability. However one must remember that GeoLocate could not perform the task, so the real comparison is GeoWatch and GeoBar.

#### *Viewers Moving Towards then Away from Broadcaster*

Participants were asked who was moving towards and then away from the broadcaster's location (Question 11). There were only correct responses per prototype, but in fact, GeoLocate and GeoBar did not provide this information (participants could note that the prototype did not provide the information). Table 4.19 presents the results for the numbers correct, the Exclusions and the Intrusions. Even though GeoLocate and GeoBar could not perform the task, there is still the chance for Intrusion Errors.

Table 4.19 Number of Participants who Correctly Identified the Viewers Moving Towards, then Away from the Broadcaster

Prototype	Correct ID: ToAway		Exclusions: ToAway				Intrusions: ToAway			
	Num	Percent	Mean	SD	Min	Max	Mean	SD	Min	Max
GeoLocate	21	100.0	na	na	na	na	0.00	0.00	0	0
GeoWatch	17	81.0	0.19	0.40	0	1	0.10	0.44	0	2
GeoBar	14	66.7	na	na	na	na	0.38	0.59	0	2

Notes: na is not applicable

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Correct: To Away* differed significantly with  $F(2,40) = 4.277$  ( $p < 0.021$ ,  $\eta^2 = 0.176$ ). Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were different ( $t(40) = 2.159$ ,  $p < 0.046$ ), that GeoLocate and GeoBar were different ( $t(40) = 3.171$ ,  $p < 0.005$ ), but that GeoWatch and GeoBar were not different ( $t(40) = 1.000$ ,  $p < 0.329$ ). Because there is only one correct response, the Exclusions are the opposite of the Correct, so the analysis is the same (and there is only one group).

A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Intrusions: ToAway* differed significantly with  $F(2,40) = 5.200$  ( $p < 0.001$ ,  $\eta^2 = 0.206$ ). Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were not different ( $t(40) = 1.000$ ,  $p < 0.329$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 2.043$ ,  $p < 0.055$ ). but that GeoLocate and GeoBar were different ( $t(40) = 2.953$ ,  $p < 0.008$ ).

The correlation for *Correct ID: ToAway* between participants were computed. Correlations involving GeoLocate had a constant level of performance, so correlations could not be computed between GeoLocate and GeoWatch or GeoBar. For GeoWatch and GeoBar,  $r = -.086$  ( $p < 0.712$ ). Prototype 1, 2 and 3 do not seem to tap common skills or cognitive abilities.

For finding the viewers who move towards and away, GeoLocate seems the best, but GeoLocate does not have the capability to assess movement. However, most participants were aware that GeoLocate could not perform the task and correctly indicated that. Furthermore, GeoBar could not perform the task (hence, similar issues). Hence, the best performance is GeoWatch simply because it is the only prototype that can perform the task.

### *Distances to Particular Viewers*

Participants were asked to find the distances to two specific individuals (Questions 12 and 13). They were coded as right or wrong. For GeoLocate, the 19 of 21 participants had the correct distances and the other participant was only correct for one of the two viewers. For GeoWatch, 20 of 21 participants (95.2%) had the correct distances and the other participant had one correct viewer, but was missing on the other. For GeoBar, 18 of 21 participants (85.7%) had both distances correct: 1 participant was wrong for both viewers, another participant had one correct viewer but missing on the other, and the final participant was wrong for both viewers. A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Correct: Distances* did not differ significantly with  $F(2,40) = 0.811$  ( $p < 0.452$ ,  $\eta^2 = 0.039$ ). Follow-up planned within-subjects *t*-tests showed that GeoLocate and GeoWatch were not different ( $t(40) = 0.000$ ,  $p < 1.000$ ), that GeoLocate and GeoBar were not different ( $t(40) = 0.899$ ,  $p < 0.379$ ), but that GeoWatch and GeoBar were not different ( $t(40) = 1.375$ ,  $p < 0.186$ ).

The correlation for *Specific Distances* between participants were computed. For GeoLocate and GeoWatch,  $r = -.073$  ( $p < 0.755$ ), for GeoLocate and GeoBar,  $r = -0.127$  ( $p < 0.584$ ) and for GeoWatch and GeoBar,  $r = 0.646$  ( $p < 0.002$ ). GeoWatch and GeoBar seem to tap a common skill or cognitive ability for this task.

For distances to specific individuals, all prototypes were the same.

### *Performance Summary*

To try to understand performance at a more general level, Table 4.20 ranks all the prototypes on each of the tasks performed. Each prototype is assigned a rank from 1 to 3 (best to worst). Ranks are based on significant difference. As such, if there were no differences in performance, then the ranks would be tied. That is, if all prototypes were the same (no overall differences), then all received a rank of 2. If some prototypes were different, then ranks were based on those that were different (ties represented by the middle of the assigned ranks). If a prototype could not perform a function, it was placed at the bottom rank.

Table 4.20 Performance Ranking of Prototypes Across Tasks

		GeoLocate	GeoWatch	GeoBar
Question Number				
1	Number Viewers	1	2.5	2.5
2	ID Viewers	1	2.5	2.5
3	My Location	2	2	2
4	Distances	1	2.5	2.5
5	Appeared	2	2	2
6	Disappeared	1	3	2
7	Closest	2	2	2
8	Furthest	2	2	2
9	Toward	2	2	2
10	Away	3	2	2
11	To and Away	2.5	1	2.5
12, 13	Specific Distances	2	2	2
	Mean	1.79	2.13	2.17
	SD	0.66	0.48	0.25
	Min	1.00	1.00	2.00
	Max	3.00	3.00	2.50

Table 4.20 also provides some summary statistics for the ranking. By this summary, GeoLocate is the best choice. However, one must remember that individual users would have personal preferences so certain features (tasks) might be relatively more important than others.

Table 4.20 also makes it clear that the differences are not large. Participants may not yet know what the location prototypes would be used for in the real world. For example, is a broadcaster ever going to want a list of all the people who viewed the broadcaster's location? Is it more likely that the want to know who is close or who is approaching? We tested both, but both might not be of equal value. Therefore, it should be noted that additional testing needs to be conducted. Participants provided valuable verbal (typed) comments, which would become a part

of the next iteration of the design cycle.

### *Affect Measures*

Upon completion of the task, participants provided ratings on a number of dimensions. Each of these was scored on a 5-point scale (from 1 to 5) with 5 indicating more agreement.

Table 4.21 provides the questions, and Table 4.22 provides the analysis of differences between responses as a function of Question.

Table 4.21 Question List for Rating Prototypes.

Quest Num	Question Content
1	The purpose of the feature was clear
2	The announcement that viewers had examined my location was easy to obvious
3	It was easy to determine if viewers had examined my location
4	It was easy to find information about viewers
5	The information provided about viewers would be useful
6	The presentation of information about viewers was understandable at first glance (intuitive)
7	It was easy to find the location of specific viewers
8	It was easy to find the identification of viewers at specific locations (distances)
9	It would be easy to continue broadcasting while checking viewer information
10	Overall the task was easy to perform
11	Overall the task was understandable
12	Overall the layout was nice
13	This feature would help me to feel more secure while broadcasting
14	This feature would remind me to reconsider my behavior about disclosing my location
15	This feature would add enjoyment to my broadcasts

Table 4.22 presents the mean rating per prototype, per question. It also reports the results of a one-way within-subjects ANOVA with three levels of Prototype, providing the  $F$  (all tests have 2.40  $dfs$ ), the  $p(F)$  and the effect size ( $\eta^2$ ). Finally, it presents the  $p(t)$  for the test of the specific differences between Prototypes (all specific tests have (1,40)  $df$ ). Note that these tests should be considered “planned” and as such, a type 1 error rate of  $\alpha = 0.05$  should be used. However, if one should desire to apply a Bonferroni correction, the actual  $p(t)$  is provided (i.e., divide 0.05 by the size of the correction and use this as the criterion).

Table 4.22 Analysis of Ratings as a Function of Prototypes.

Quest Num	Prototype			ANOVA			Prototype Comparisons		
	1	2	3	<i>F</i>	<i>p(F)</i>	$\eta^2$	1 vs 2	1 vs 3	2 vs 3
	GeoLocate	GeoWatch	GeoBar						
1	3.95	4.33	4.24	1.677	0.200	0.077	0.104	0.110	0.705
2	3.91	3.81	4.05	0.564	0.573	0.027	0.629	0.526	0.366
3	3.76	3.95	3.81	0.261	0.771	0.013	0.479	0.825	0.673
4	4.14	3.95	4.05	0.222	0.802	0.011	0.550	0.680	0.760
<b>5</b>	<b>3.86</b>	<b>4.05</b>	<b>4.33</b>	<b>3.938</b>	<b>0.027</b>	<b>0.165</b>	0.296	<b>0.021</b>	0.055
6	4.05	4.19	4.14	0.102	0.904	0.005	0.679	0.741	0.890
7	4.05	4.24	4.24	0.241	0.787	0.012	0.605	0.493	1.000
8	4.48	4.38	4.43	0.096	0.909	0.005	0.666	0.815	0.841
<b>9</b>	<b>3.95</b>	<b>3.14</b>	<b>4.38</b>	<b>8.724</b>	<b>0.001</b>	<b>0.304</b>	<b>0.023</b>	0.131	<b>0.001</b>
10	4.10	4.00	4.43	1.782	0.181	0.082	0.705	0.167	0.083
11	4.38	4.24	4.43	0.579	0.565	0.028	0.480	0.803	0.258
12	4.14	4.10	4.57	2.241	0.119	0.101	0.841	0.071	0.106
13	3.57	3.86	4.05	2.643	0.084	0.117	0.229	0.056	0.214
14	4.29	4.29	4.43	0.741	0.483	0.036	1.000	0.329	0.267
15	4.10	3.95	4.10	0.397	0.675	0.019	0.329	1.000	0.545
Mean	4.05	4.03	4.24						
SD	0.23	0.30	0.21						
Min	3.57	3.14	3.81						
Max	4.48	4.38	4.57						

Note that all the prototypes received relatively high ratings (the center of the scale was 3 for neutral), and most prototypes received the same ratings. However, Questions 5 and 9 were different. GeoBar was rated much higher on Question 5 (information would be useful), and GeoBar was also rated much higher on Question 9 (easy to continue broadcasting). Note that



GeoWatch was rated low on this question, which is not surprising given that the prototype takes over the entire screen to present the information.

Table 4.22 also presents the mean, sd, minimum and maximum rating for each prototype across all questions. While the choice of prototype would be based, to some degree, on personal preferences, note that GeoBar has a higher overall rating, and a lower standard deviation. It also has the highest minimum. Simplistically, GeoBar would be the best to pursue overall.

After working with all three prototypes, participants were asked to rank the three prototypes from Best through Middle to Worst. Table 4.23 presents the number of times each was ranked Best, Middle or Worst, as well as the mean ranking. For the analysis, Best was coded as 1, Middle as 2 and Worst as 3.

Table 4.23 Rankings of Prototypes.

	GeoLocate	GeoWatch	GeoBar
Best	3	7	11
Middle	9	9	8
Worst	8	5	2
mean	2.25	1.90	1.57
sd	0.72	0.77	0.68

For the analysis, Best was coded as 1, Middle as 2 and Worst as 3. Tied ranks were coded at the midpoint (e.g., Best, Middle, Middle was coded as 1, 2.5, 2.5). A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Ranking* differ significantly with  $F(2,40) = 2.512$  ( $p < 0.038$ ,  $\eta^2 = 0.151$ ). Follow-up planned within-subjects *t*-tests showed that the ranks assigned to GeoLocate and GeoWatch were not different ( $t(40) = 1.449$ ,  $p < 0.162$ ), and that GeoWatch and GeoBar were the same ( $t(40) = 1.165$ ,  $p < 0.258$ ). but that GeoLocate and GeoBar were different ( $t(40) = 2.760$ ,  $p < 0.012$ ).

Finally, participants were asked a number of questions pertaining to the general utility of the location prototypes. The first was “Would you be likely to install an app that has this feature on your phone or video broadcasting device?”: 85.7% (18) said “yes” while the remaining 14.3% (3) said “Maybe”. Participants were asked “If an app like this was installed on your phone or video broadcasting

device, would you use it?": 47.6% (10) said "Yes regularly" while 52.3% (11) said "Maybe / Not sure". One participant provided a verbal response ("Maybe: I would use it if it runs smoothly without any latency or lags") that was consistent with and coded as "Maybe / Not sure").

Participants were asked, "This type of app only provides information about people who viewed your location. Who would you want to know about?". The first response option was "Only those people who are in my city." and it was endorsed by 42.9% (9) participants. The second response option was "Only viewers who are within a specific preset distance from my location." and it was endorsed by 33.3% (7) participants. The third and final response option was "Any viewers from any location in the world." and it was endorsed by 52.9% (11) participants. The level of endorsement did not differ with  $F(2,40) = 0.559$  ( $p < 0.476$ ,  $\eta^2 = 0.027$ ). Options 1 and 3 were negatively correlated across participants with  $r = -.716$ , ( $p < 0.0005$ ). Those who like Option 1 do not like Option 3. However, Option 1 was not correlated with Option 2 ( $r = -.204$ ,  $p < 0.375$ ) and Option 2 was not correlated with Option 3 ( $r = -.134$ ,  $p < 0.560$ ).

Participants were asked, "Which features of an application are important?" Table 4.24 presents the response options and the proportion of endorsement for each.

Table 4.24 Which Features are Important?

	<i>N</i>	%
the ability to monitor people who start to view your location	21	100.0
the ability to monitor people who stop viewing your location	6	28.6
the ability to see the closest person	20	95.2
the ability to see the furthest person	7	33.3
the ability to see the people moving toward your location	19	90.5
the ability to see the people moving away from your location	10	47.6

Generally, participants want the ability to see who is viewing their location, but most do not care about those who have stopped. Proximity is also a factor. The levels of endorsement for the 6 options differed significantly with  $F(5,100) = 21.074$  ( $p < 0.0005$ ,  $\eta^2 = 0.513$ ). Options 1 and 3 were negatively correlated across participants with  $r = -0.716$ , ( $p < 0.0005$ ). Follow-up tests indicated that Options 1, 3, and 5 were endorsed equally often. Option 2, 4 and 6 were endorsed

equally often. Finally, Options 1, 3, and 5 were endorsed more often than Options 2, 4, and 6. The correlations between the options are presented in Table 4.25.

Table 4.25 Correlations between the Options for Which Features are Important?

	1	2	3	4	5	6
1	1.000	na	na	na	na	na
2		1.000	0.141	<b>0.447</b>	0.205	0.241
3			1.000	0.158	<b><i>0.689</i></b>	0.213
4				1.000	0.229	<b>0.539</b>
5					1.000	0.309
6						1.000

Notes: **Bold** =  $p < 0.05$ ; **Bold-Italic** =  $p < 0.01$ ;  $N = 21$  for all comparisons.

These are equivalent to phi-correlations.

NA = the correlation could not be computed because everyone endorsed Option 1

Note that Options 3 and 5 are highly correlated and that Options 2, 4, and 6 are correlated. However, options 3 and 5 are not strongly correlated with Options 2, 4, and 6. There may be subgroups.

In general, one of the most interesting observations is that Prototype 3 (GeoBar) was the most preferred by participants (Table 4.23), and yet it did not demonstrate the highest level of performance (Table 4.20). However, participants were *not* provided feedback about performance. Such feedback might alter ratings.

#### 4.4.3.1.1 Feedback from Participants

Comments can be used in the design of the next set of prototype for future development.

## Likeability

Table 4.26 Participants' Feedback about Location Viewers Prototypes: Likeability

GeoLocate	GeoWatch	GeoBar
<ul style="list-style-type: none"> <li>• “Animation”</li> <li>• “Showing a list of people who are near by me and their distance”</li> <li>• “A simple UI.”</li> <li>• “Keeping me informed about the where of my viewers”</li> <li>• “The task was simple laid for even non-technical person to understand”</li> <li>• “Easy to know usernames with their corresponding icons.”</li> <li>• “The total number of viewers was pretty obvious”</li> <li>• “Clear representation of things/info”</li> <li>• “the way my viewers are shown graphically and how the number of them are reduced based on my location.”</li> </ul>	<ul style="list-style-type: none"> <li>• “Picture of users who are nearby”</li> <li>• “The Radar concept is very good”</li> <li>• “Knowing users coming close and moving away”</li> <li>• “The task made it easier to understand about the developed feature”</li> <li>• “It shows in 2 dimensions. easy to see distance, group of people”</li> <li>• “It was easy and visually cognitive.”</li> <li>• “more fun”</li> <li>• “give me more secure feeling and a better understanding”</li> <li>• “I love the way of viewing the viewers. I love how I can see them moving in a real time manner.”</li> <li>• “It is easy to navigate and view users around me”</li> </ul>	<ul style="list-style-type: none"> <li>• “Animation”</li> <li>• “The time line in the top of the screen was very good”</li> <li>• “It gives more are to see my broadcasting video”</li> <li>• “The fact that I know which users are coming close and going far and by how much distance.”</li> <li>• “It was easy to understand and perform This layout was better in terms of usability easiness”</li> <li>• “what i like here was that i can see list of people all above and easier i can see their distance, in addition, it was enjoyable for me to know which 2 people are at the same position.”</li> </ul>

GeoLocate	GeoWatch	GeoBar
<ul style="list-style-type: none"> <li>• “I like the display of the users and how the circles are popping up and catching my attention even if I was involved in a talk with the viewers.”</li> <li>• “It as simple to operate”</li> <li>• “Being able to organize followers meet up.”</li> <li>• “If used with only people I know and trust my friends could come closer to me and join the broadcast.”</li> <li>• “Standard way of display the viewers so it's easy to understand and use from the first time”</li> <li>• “I could tell how many viewers are viewing my broadcast right away”</li> <li>• “Precise, organized (sorted), one tab view to see the entire list of viewers with their info”</li> </ul>	<ul style="list-style-type: none"> <li>• “showing the restricted boundary and the people moving inside.”</li> <li>• “I also liked that if more than one person was in a spot”</li> <li>• “the icon itself turned into the number- I think the second task with the bar would benefit from that idea- instead of the big red "I"”</li> <li>• “more interaction way of displaying user information.”</li> <li>• “color coding for the viewers easy to see who close to me and who is far, obvious to click on the eye to see the radar”</li> <li>• “Best visualization. Solve the problem on how to display when there are many viewers.”</li> <li>• “I could see the relative directions of my viewers”</li> <li>• “makes me watch all of the people in surrounding”</li> </ul>	<ul style="list-style-type: none"> <li>• “It is very easy for me to know who is exactly closer to my location without even clicking on the information about the viewer.”</li> <li>• “I can visually recognize who is closer to my location”</li> <li>• “The icons were easy to see and access and the "I" was great for if two were too close to touch separately”</li> <li>• “the layout of user list was simple and easy to understand”</li> <li>• “It doesn't interfere with the broadcast yet, shows user location in interaction way.”</li> <li>• “i can view the infor without any interruption of the broadcast. It is 1 dimension”</li> <li>• “I can see my viewer's locations and also my broadcast at the same time.”</li> <li>• “less distracting compared to other two applications”</li> </ul>

## Dislikeability

Table 4.27 Participants' Feedback about Location Viewers Prototypes: Dislikeability

GeoLocate	GeoWatch	GeoBar
<ul style="list-style-type: none"> <li>• “See who are coming near and going away was tough.”</li> <li>• “not interactive and fun as other apps”</li> <li>• “I can't view my location”</li> <li>• “The long list of name that appear once. What if I have over a thousand people viewing my location?”</li> <li>• “Sometimes unresponsive up swipe list showing people around that too in jumble order. I am not able to make who is near and far easily”</li> <li>• “It does not show the name of the person who is moving when the app shows the person is moving.”</li> <li>• “Not knowing the exact location of followers moving towards me on a map.”</li> </ul>	<ul style="list-style-type: none"> <li>• “I cannot see my video”</li> <li>• “keeping track of all user when they are all moving at the same time.”</li> <li>• “Need to click and list appears of users”</li> <li>• “Separate screen to view info”</li> <li>• “The viewer location window blocks the view of my broadcast”</li> <li>• “the color dots with no user image.”</li> <li>• “have to stop broadcast and look at the map”</li> <li>• “I am not able to see what I am broadcasting when I am viewing the locations of my viewers.”</li> <li>• “Cannot broadcast properly while using the app”</li> <li>• “Having to reload a couple of times.” <i>A drawback of the software used to design the prototype</i></li> </ul>	<ul style="list-style-type: none"> <li>• “Time line size was small”</li> <li>• “little space with many icons. if many viewer, it could be hard to see”</li> <li>• “I cannot see in which direction they are located from me.”</li> <li>• “how viewers' pictures overlap when there are more than one viewer is close to each other or in the same location.”</li> <li>• “Also "i" button in app starts showing information about person in sequence so what if i want to know something about 10th person in very go. It will take "i" button at least 10 hop to reach there that can distract broadcaster.”</li> <li>• “Refreshing to gain or retrieve the disappeared viewers.”</li> <li>• “the "i" icon is red gave me a sense of danger.”</li> </ul>

GeoLocate	GeoWatch	GeoBar
<ul style="list-style-type: none"> <li>• “App does not show users who move away from my location. Also does not show the location of users relative to each other.”</li> <li>• “I could not say who joined my list of viewers or which viewer stopped viewing.”</li> </ul>	<ul style="list-style-type: none"> <li>• “Tedious, continually need to repeat app” <i>A drawback of the software used to design the prototype</i></li> <li>• “I have to click and then to figure out who is actually moving in”</li> </ul>	<p>–</p>

### *Usefulness*

Participants were asked whether the Location Viewers Feedback feature was useful, and they commented as following:

1. Notifying about the distance of location viewers. Awareness of people around a broadcaster P(47)
2. “Get noticed when someone moving close to my location.” P(7).
3. “I am always concerned about who is viewing my live broadcasts and if any of my viewers know me in person. This feature will let me be more aware of this situation” P(5).
4. “Track number of people involved in or participating in any given Event I am hosting (Rallies, Marathons, Educational)” P(12).
5. “When you are waiting for a person to come or want to check whit whom your friend is coming is enjoyable.” P(25).
6. "While broadcasting I would be focusing on socializing with others rather than monitoring who comes or leaves, so notification helps me follow who is coming close and leaving” P(14).
7. “The notification was informative” P(22).
8. “Depends on why the user is broadcasting” P(90).
9. “I’ll get notified and I can block or hide that person from the list of viewer.” P(17).
10. “The notification is not as useful as the graphic” P(82).
11. “I think people would use it for fun not for safety. They would use to it say "I had a viewer from France today" or "when I told everyone I was at the park three people came closer to

me!"” P(36).

12. “Keep me conscious about my location privacy.” P(74).
13. to find the number of viewer from particular location. P(1).
14. “Provides information about taking care of my safety.” P(10).

#### 4.4.3.1.2 Suggestions for Location Viewers Feedback Designs

The specific suggestions for each prototype are provided below. These are not ordered in any specific way. Participants provided general suggestions and feedback as well. These suggestions can be used in the design of the next set of prototype for future development (see Table 4.28).

Table 4.28 Participants’ Suggestions for Location Viewers Feedback Designs

<b>Prototype</b>	<b>Comments</b>
<b>GeoLocate</b>	<p>“Font size”, “Showing the name of viewers who are moving toward location, not only their profile photos”, “Showing details about the viewer and previous location of that viewer”, “Changing the order of viewers in the list based on the closet to the furthest”, “Having a particular color of circle for people moving away from location to provide a sense of concern of what data is shared with all. “Having a profile photo pop up for the individuals closest to the location”, “ Improve the touch screen to avoid trying many times.” “My location’ icon can be on one side of the screen and when viewers get closer, their profile photos slowly move across to location instead of moving over many times.”,</p> <p>“The touch wasn’t sensitive enough- I had to try many times- also the bubble that said ‘my location’ looks like I should be able to open it. “Use map to show viewers.” “Representing the viewers who are moving toward the location with a green color, and those who are moving away with a red color.”</p>
<b>GeoWatch</b>	<p>“Make the range of viewers wider, and show the number of viewers outside. Maybe this with a small statistic or a bubble chart show the</p>



Prototype	Comment
<b>GeoWatch</b>	<p>distance”, “Make a zoom in a map or a radar to see the viewers instead of clicking”, “The radar can be more transparent to show what is broadcasting at the same time.”, “Use a split screen or a lower hover tab to avoid making the radar covering the broadcast.”, “Show the viewers’ information while they are moving.”, “Adding a particular color for people who are in the same location to notify about the same proximity.”, “Include the name of a place, where the viewer is, with the distance”, “Design the radar to be smaller and moveable so that the broadcaster can shrink it while broadcasting.”, “Customize the design for the security level e.g., Not showing location when broadcasting at work, but show the location at public places” “210ustomization for the security level. Eg: broadcasting at work place do not necessarily need the viewrs locations, however public broadcasts may require the user location feature.”, “Include the name of the city on the same radar above ‘N’” , “Its looks perfect to me as it is”</p>
<b>GeoBar</b>	<p>“Scale (GeoBar) size”, “How to manage large numbers of viewers’ appearance.”, “Show the distance and direction of the viewer.”, “Instead of having an (i) to show there two viewers or more, provide an icon of a number of viewers located at a given distance.”, “Provide an easy access to block viewers from seeing the broadcast or location”, “Provide the feature of selecting who can see the location.”, “An automatic display of viewers who are moving toward the broadcaster.”</p>
<b>All Prototypes</b>	<p>“A massive group of viewers could be grouped by average distance or in ranges.”, “Adding a feature of statistics that save how many viewers are watching and send this information to a sponsorship to add ads during broadcasting”, “Incorporating the three apps into a single app”, “Combine GeoWatch and GeoBar”, “Combination of radar and bar would be great”, “If all features of the 3 apps are incorporated into a single app it would be brilliant.”, “Meaning the user location tracking interface does not interrupt the broadcasting and still me informative in displaying user distance and</p>

Prototype	Comments
<b>All Prototypes</b>	photo” “Having the option to hide the location”, “Showing a profile photo of a viewer, name and distance at once without clicking.”, “Using profile’s photo to represent the user instead of using dots.”, “Adding a feature of blocking anyone the broadcaster does not want to let them to see his location.”, “A hybrid system including the features of GeoWatch and GeoBar, and based on the user preference the location system could be change to radar based or linear (List).”

Note that some of the comments for each app are addressed by other apps. Because of the counterbalancing of presentation, some participants had not seen the features of other apps before making these comments. In addition, note that many comments are simply not possible given the available dimensions of a typical cell phone. For example, “Include the name of a place, where the viewer is, with the distance” would not be possible, and would not extend to more than a few location viewers

Note that, in the all prototypes section, many advocated a combination of the features of all three prototypes.

#### **4.4.3.2 Visual Privacy Awareness Prototypes (Mood-to-Mood, Appearance-to-Mood, Appearance-Directly)**

The analysis of the second experiment reduced to the analysis of the responses to 13 questions about the prototype. The particular questions are shown in Table 4.29. Upon completion of the task, participants provided ratings on a number of dimensions. Each of these was scored on a 5-point scale (from 1 to 5) with 5 indicating more agreement. Table 4.29 provides the questions, and Table 4.30 provides the analysis of differences between responses as a function of Question.

Table 4.29 Question List for Rating the Privacy Prototypes.

Quest Num	Question Content
1	The task was easy to perform
2	The task was understandable.
3	The overall layout was nice.
4	Imagine if you were to be in a good mood (e.g., happy, relaxed, calm): a) The task would be easy to perform.
5	Imagine if you were to be in a good mood (e.g., happy, relaxed, calm): b) The task would be understandable.
6	Imagine if you were to be in a bad mood (e.g., frustrated, angry, sad): a) The task would be easy to perform.
7	Imagine if you were to be in a bad mood (e.g., frustrated, angry, sad): b) The task would be understandable.
8	Imagine if you were to be intoxicated (i.e., drunk, inebriated, using street drugs): a) The task would be easy to perform.
9	Imagine if you were to be intoxicated (i.e., drunk, inebriated, using street drugs): b) The task would be understandable.
10	This feature would help me to feel more secure about my broadcasting.
11	This feature would help me to be more aware of my behavior while broadcasting.
12	This feature would help me to reconsider my behavior when broadcasting.
13	This feature would add enjoyment to my broadcasting.

Table 4.30 presents the mean ratings per prototype, per question. It also reports the results of a one-way within-subjects ANOVA with three levels of Prototype, providing the  $F$  (all tests have 2,40  $dfs$ ), the  $p(F)$  and the effect size ( $\eta^2$ ). Finally, it presents the  $p(t)$  for the test of the specific differences between Prototypes (all specific tests have (1,40)  $df$ ). Note that these tests should be considered “planned” and as such, a type 1 error rate of  $\alpha = 0.05$  should be used. However, if one should desire to apply a Bonferroni correction, the actual  $p(t)$  is provided (i.e.,

divide 0.05 by the size of the correction and use this as the criterion).

Table 4.30 Analysis of Ratings as a Function of Prototypes (Mood-to-Mood, Appearance-to-Mood, Appearance-Directly)

Quest Num	Prototype			ANOVA			Prototype Comparisons		
	4	5	6	<i>F</i>	<i>p(F)</i>	$\eta^2$	4 vs 5	4 vs 6	5 vs 6
	Mood-to- Mood	Appearance- to-Mood	Appearance- Directly						
1	4.24	4.33	4.62	2.997	0.061	0.130	0.605	<b>0.042</b>	0.030
2	4.14	4.33	4.33	0.399	0.674	0.020	0.428	0.463	1.000
3	4.19	4.29	4.38	0.305	0.739	0.015	0.629	0.493	0.715
4	4.24	4.52	4.48	0.855	0.433	0.041	0.162	0.424	0.815
<b>5</b>	4.29	4.38	4.43	0.323	0.726	0.016	0.428	0.505	0.815
6	3.52	3.90	3.95	1.299	0.284	0.061	0.189	0.242	0.833
7	3.57	3.71	3.76	0.371	0.692	0.018	0.419	0.463	0.853
<b>8</b>	<b>2.38</b>	<b>3.33</b>	<b>3.43</b>	<b>9.867</b>	<b>0.000</b>	0.330	<b>0.000</b>	<b>0.003</b>	0.715
<b>9</b>	<b>2.71</b>	<b>3.38</b>	<b>3.33</b>	<b>4.221</b>	<b>0.022</b>	0.174	<b>0.023</b>	<b>0.015</b>	0.858
10	3.95	4.10	4.19	0.463	0.633	0.023	0.602	0.309	0.705
11	4.05	4.33	4.14	0.842	0.438	0.040	0.267	0.576	0.446
12	4.00	4.43	4.14	1.765	0.184	0.081	0.143	0.419	0.229
13	3.62	3.76	3.43	0.716	0.495	0.035	0.624	0.446	0.285
Mean	3.76	4.06	4.05						
SD	0.60	0.40	0.43						
Min	2.38	3.33	3.33						
Max	4.29	4.52	4.62						

Firstly, note that questions 1, 2, 3, 4, 6, 10, 11, and 12 all received relatively high ratings. In addition, these questions did not show any differences between prototypes. However, Questions 6, 7, 8, and 9 received much lower overall ratings.

Table 4.30 also presents the Mean, SD, Minimum and Maximum rating for each prototype across all questions.

After working with all three prototypes, participants were asked to rank the three prototypes from Best though Middle to Worst. Table 4.31 presents the number of times each was ranked Best, Middle or Worst, as well as the mean ranking. For the analysis, Best was coded as 1, Middle as 2 and Worst as 3.

Table 4.31 Rankings of Prototypes.

	Mood-to-Mood	Appearance-to-Mood	Appearance-Directly
Best	7	5	10
Middle	5	13	5
Worst	9	3	6
mean	2.10	1.90	1.81
sd	0.89	0.62	0.87

For the analysis, Best was coded as 1, Middle as 2 and Worst as 3. Tied ranks were coded at the midpoint (e.g., Best, Middle, Middle was coded as 1, 2.5, 2.5). A one-way within-subjects ANOVA (3 levels of Prototype) showed that the mean performance for *Ranking* did not differ significantly with  $F(2,40) = 0.351$  ( $p < 0.706$ ,  $\eta^2 = 0.017$ ). Follow-up planned within-subjects *t*-tests showed that the ranks assigned to Mood-to-Mood and Appearance-to-Mood were not different ( $t(40) = 0.686$ ,  $p < 0.500$ ), that Mood-to-Mood and Appearance-Directly were not different ( $t(40) = 0.726$ ,  $p < 0.477$ ), and that Appearance-to-Mood and Appearance-Directly were not different ( $t(40) = 0.162$ ,  $p < 0.873$ ).

The prototype with the highest number of “Best” ratings is Appearance-Directly, and prototype with the highest number of “Worst” ratings is Mood-to-Mood.

Finally, participants were asked a number of questions pertaining to the general utility of the location prototypes. The first was “Would you be likely to install an app that has this feature on your phone or video broadcasting device?": 57.1% (18) said “yes”, 33.3% (7) said “Maybe”, and 9.5% (2) said “No”. Participants were asked “If an app like this was installed on your phone

or video broadcasting device, would you use it?": 47.6% (10) said "Yes regularly", 28.6% (6) said "Maybe / Not sure", and 23.8% said "No".

Participants were asked if they preferred blurring, hiding or neither as a means of obscuring their own faces. Blurring was endorsed by 14.3% (39) of participants, hiding was endorsed by 23.81% (5) participants, and neither hiding nor blurring was endorsed by 61.9% (13) of participants. Participants were asked if they preferred blurring, hiding or neither as a means of obscuring the face of others in the background. Blurring was endorsed by 42.9% (9) of participants, hiding was endorsed by 38.1% (8) participants, and neither blurring nor hiding was endorsed by 19.0% (4) of participants.

#### 4.4.3.2.1 Feedback from Participants

Comments can be used in the design of the next set of prototype for future development.

#### *Likeability*

Table 4.32 Participants' Feedback about Visual Privacy Prototypes: Likeability

Mood-to-Mood	Appearance-to-Mood	Appearance-Directly
<ul style="list-style-type: none"> <li>• "It will be helpful for people who drunk and broadcast."</li> <li>• "It requires a higher level of consciousness, so an intoxicated user may find it hard to make a perfect match and this will let the app set a higher level of privacy"</li> <li>• "Good options, matching is easy"</li> </ul>	<ul style="list-style-type: none"> <li>• "An easy way to choose the privacy setting"</li> <li>• "It protects me from presenting bad behaviour"</li> <li>• "It was easy and understandable"</li> <li>• "Safety filter protects our identity from false hands"</li> <li>• "It can hide my appearance when I am in a negative mood"</li> </ul>	<ul style="list-style-type: none"> <li>• "Provide an easy preference in choosing the privacy level"</li> <li>• "It shows me what kind of category I will present my face"</li> <li>• "The reminder based filter make oneself to think twice"</li> <li>• "It gives a subtle reminder of who may be watching me"</li> </ul>

Mood-to-Mood	Appearance-to-Mood	Appearance-Directly
<ul style="list-style-type: none"> <li>• “this application automatically predicts the mood of the people by choosing the right or wrong face.”</li> <li>• “the idea of the blurring”</li> <li>• “It helps to control my emotions and behavior”</li> <li>• “protects my identity and I would probably use it even if i am in a happy mood for privacy purposes”</li> <li>• “Automatically selecting filter is a great idea as sometime you forget to select filter but selecting mood can save you in some place.”</li> <li>• “help me reconsider my actions”</li> <li>• “Great idea for when you're drunk or angry and not making good choices in social media”</li> <li>• “easy to understand”</li> </ul>	<ul style="list-style-type: none"> <li>• “easier to perform than app Mood-to-Mood”</li> <li>• “Gives you choices for mood selection”</li> <li>• “this one seems to me like a double check, one from the person who is the user and the other one which is performed automatically.”</li> <li>• “Its informative”</li> <li>• “The reminder notification”</li> <li>• “The way we match different mood with level of filter we require.”</li> <li>• “Could be used in specific cases.”</li> </ul>	<ul style="list-style-type: none"> <li>• “can hide face identification of user”</li> <li>• “Simple, easy to use”</li> <li>• “i like this one because i have the ability to choose which one i like to be presented by.”</li> <li>• “It's easier than the previous app 4 &amp; 5 in terms of choosing the mood. Instead of matching and dragging”</li> <li>• “doesn't choose for me "force me" but it allows me to choose what I want”</li> <li>• “I can chose were to put my real face”</li> <li>• “The choice is clear and the reason is clear”</li> <li>• “it remind me of the type of audience that might be seeing my broadcast.”</li> </ul>

## Dislikeability

Table 4.33 Participants' Feedback about Visual Privacy Prototypes: Dislikeability

Mood-to-Mood	Appearance-to-Mood	Directly- Appearance
<ul style="list-style-type: none"> <li>• “The icons on the right side were too small”</li> <li>• “Would be annoyed when intoxicated.”</li> <li>• “sometimes complicated”</li> <li>• “it might be difficult for those that cannot correctly interpret emojis”</li> <li>• “Difficult to match shapes due to distance, unclear what matching does”</li> <li>• “The icons didn't slide which made it hard to match”</li> <li>• “could have been more automatic.”</li> </ul>	<ul style="list-style-type: none"> <li>• “More option needed to show the emotions”</li> <li>• “I think it could emphasis more about a bad possible behave”</li> <li>• “It is up to the user to choose his/her mood. So a user who is very drunk may choose the mood happy by mistake.”</li> <li>• “Sliding action for selecting mood is finicky”</li> <li>• “interface can be improved”</li> </ul>	<ul style="list-style-type: none"> <li>• “Friends, Family and co-worker should be given as option not in a random way”</li> <li>• “the categories past too fast”</li> <li>• “It does not hide the user name of the broadcaster when he/she is in a negative mood”</li> <li>• “since it gives me the freedom to choose, it would lack the " suggestion feature " that app 4&amp; 5 have”</li> <li>• “I may want to seperate my family related information from workers”</li> <li>• “related information”</li> </ul>

### 4.4.3.2.2 Suggestions for the Visual Privacy Awareness Designs

There were also specific suggestions on each visual privacy prototype as well as general suggestions for all three. Comments can be used in the design of the next set of prototype for



future development (see Table 4.34)

Table 4.34 Participants' Suggestions for Visual Privacy Awareness Designs

<b>Prototype</b>	<b>Comments</b>
<b>Mood-to-Mood</b>	"Icon size", "Details could be enhanced to not commit errors." <i>A drawback of the software used to design the prototypes</i>
<b>Mood-to-Appearance</b>	"Include more mood states"
<b>Appearance-Directly</b>	"Use icons to represent the type of viewers (e.g., family, friends, etc.) when warning the user about the viewers."
<b>All Prototypes</b>	"Letting the system asking about current mood, and provide recommendation about showing face.", "Hiding the user name when the user is in a negative mood.", "Screen size", "Having an option blur or hide the people around", "Optimize matching mood.", "Having filter options of visual privacy to select for each group of viewers", "Use icons to represent the type of viewers (e.g., family, friends, etc.) when warning the broadcaster about the viewers."

## 4.5 Discussion

### 4.5.1 Participants Demographic

There were 16 males and 5 females participated in the two experiments. Their ages ranged from 24 -43 years, but most were below 28. Most (86%) had graduate degrees. Their comfort of technology ranged from comfortable to very uncomfortable, and their knowledge of computer security ranged from minimal to expert but 95% were good or expert. All participants currently resided in the Halifax region, and most were associated with Dalhousie University.

## **4.5.2 Live Video Broadcasting Use**

In this section we discuss our participants': (a) background, (b) use of, and (c) perception of privacy issues with live video broadcasting apps.

Interestingly, the most prototype that respondents used was Periscope. This is likely because it offers a private feature that participants specifically noted using. This implies that the respondents do care about their privacy. However, almost all participants use public BCs at least some of the time which can raise privacy issues. Privacy issues are more of a concern if those BCs are spontaneous. For the current sample, respondents broadcast mostly to promote events or to maintaining relationships with online and offline friends. They do so from home and from public places (or at parties).

Respondents indicated that location and inappropriate behavior were the most sensitive information that they would like to keep private. In this study, we tested three different prototypes designed to provide a mechanism to allow the broadcaster be aware of those who are viewing the broadcaster's location. Inappropriate behavior needs a definition as it could carry many meanings. We can conclude that inappropriate behavior would be based on visual appearance, but there might be a verbal component as well (e.g., profanity). Data also indicates that participants are aware of the fact that mood is an issue for "inappropriate behavior" (Table 4.8). In this study, we tested three different prototypes designed to "remind" the broadcaster of the importance of mood during broadcasting. Two of these prototypes set default levels of privacy based on the self-declared mood of the broadcaster.

## **4.5.3 Comparison of Location Viewers Feedback Prototypes**

In this section we compare the results of the three Location Viewers Feedback prototypes, GeoLocate, GeoWatch and GeoBar.

### **4.5.3.1 Attention**

Attention on Notification is a main component in the design of each prototype (except GeoBar). The notification indicates the number of viewers who have examined the broadcaster's location

(hereafter: location viewers). We asked “In total, How many users are viewing your location?”. Results showed that GeoLocate had a higher number of correct answers than GeoWatch and GeoBar, which were the same. This likely happened because GeoLocate remains hidden when no viewers are checking the location. The notification only appears *after* viewers starting to examine the location. Thus, this makes the notification salient. Furthermore, once there are location viewers, the GeoLocate notification will continuously grow and shrink. GeoWatch starts with a grey icon with an embedded 0 (No Viewers) implying no viewers. When there are location viewers, the color changes to red and the icon blinks. This may simply not be as noticeable. Due to the different graphical representation, GeoBar does not have a notification per say. There is a constant static presentation of the number of location viewers: that the number might not be noticeable enough. Human visual perception is attracted to change. The bigger the change is the higher the attraction.

#### **4.5.3.2 Ease of Use/Ease of Finding Information**

To assess the Ease of Use (ease of finding information about location viewers), participants had to identify all locations viewers, so we asked “Who viewed your location?”. Previously noted the correlation of Correct ID. The fact that none are significant implies the participants with the highest performance on GeoLocate were not necessarily the highest on GeoWatch or GeoBar (i.e., they could have been the highest, the lowest, or in the middle), and those with the highest on GeoWatch were not necessarily the highest on GeoBar. The fact that all are low (“small”) regardless of significance, implies that the different prototypes tap different skills rather than some common component such as “attention to detail” or “visual acuity”. GeoLocate presents all location viewers in a list, in one fixed place. One click shows all the viewers. This makes it easy to glance at the entire list. GeoWatch, and GeoBar use a more dynamic presentation: Location viewers may be stationary, or moving; they may appear or disappear. To obtain information about a particular location viewer, the broadcaster must click on the associated icon. Thus it is more difficult to see information about all the location viewers because each must be clicked in turn. To succeed, the broadcaster must remember which had been checked, and if they are moving, this might not be easy. However, in a real world situation, at the time of broadcasting, a

broadcaster would not likely want to check all location viewers. The broadcaster might want to check the closest, or those who are moving closer.

#### **4.5.3.3 Understandability and Clarity**

Parts of the Ease of Use are understandability and clarity. Participants were asked “Who is the closest to your location?” and “Who is the furthest from your location?” to identify the closest and furthest viewers (these features are static). The three prototypes used graphically different in representations for the closest, but the statistics indicated that all three prototypes had the same performance (about 80% for the closest and about 85% for the furthest). Exclusion and intrusion error rates were the same. Furthermore, performance for GeoWatch and GeoBar were moderately correlated. This is probably because of the visual clues: For the closest location viewer, GeoWatch had a red color dot placed close to the broadcaster's location while GeoBar had a circular photo profile placed close to the broadcaster's location. These are likely easy to notice. With GeoLocate, the broadcaster had to go through a list of viewers to find the one that was closest. The list was not organized by distance, which, from observation, seen to be what participants expected. With regard to furthest viewers, despite the different interfaces, performance on these basic tasks was the same.

As an expanded version of the closest and furthest task, or as an extension of the task of identifying location viewers, we asked “Where are the viewers of location located?” to identify the distances to all location viewers. Performance was not high, and was highest for GeoLocate at only 41% (the others were 14% and 5%). However, the analysis used a stringent criterion for success, and the actual data was quite confusable. There may have been issues with the wording of the question: “Where are the viewers of location located?” A better question might have asked: “How far are the viewers located from your location?” Nonetheless, the same participants completed the same task with all three prototypes (hence, each had the same interpretation to the question), and the order of prototypes presentation was counterbalanced, so the differences between the tasks are real. GeoLocate was likely the highest because it presents all the information in a single list. The other two prototypes require the broadcaster to move through each individual location viewer in turn. This is slow and error prone. A complication for this task

is that same location viewers were dynamic. This would have had more effect on the GeoWatch and GeoBar prototypes than on the GeoLocate. A better way of presenting viewers information should be developed for dynamic viewers.

We also assessed the dynamic aspects of the interface: location viewers appearing “Who suddenly appeared on your list of viewers (started to view your location)?”, location viewers disappearing “Who suddenly disappeared from your list of viewers (stopped viewing your location)?”, location viewers moving toward “Who is moving toward your location?”, location viewers moving away “Who is moving away from your location?” and location viewers moving toward and away “Who moved towards and then away from your location?”. GeoLocate did not provide dynamic information (though it did specifically indicate that viewers were moving toward the broadcaster). As such, at best, participants could only correctly recognize that the information was not available. In fact, for GeoLocate, about 43% of participants incorrectly identified location viewers who appeared, 19% incorrectly identified location viewers who disappeared, and 9% incorrectly identified location viewers moving away from the broadcaster (none were incorrect with moving toward and away). This represents a serious misinterpretation of the capabilities of the GeoLocate. GeoWatch and GeoBar had comparable percentages of correct answers for appearing (about 60%), disappearing (about 53%) and moving toward (about 60%). GeoBar could not assess location viewers who were moving then away.

The layouts for location viewers in GeoWatch and GeoBar were different. GeoWatch used a radar screen with colored objects. GeoBar used profile photos of viewers along a bar. GeoWatch identified the appearance of location viewers with a sudden bouncing circle. GeoBar was more muted: The new location viewer simply appeared. However, for appearances, performance was the same (about 60%), and exclusion and intrusion error rates were the same. For disappearances, both simply erased the representational icon. For both, performance was the same (about 53%). For location viewers moving toward the broadcaster, GeoLocate and GeoWatch were about the same (about 71%) and higher than GeoBar (about 57%) but the difference was not significant. It is likely that performance is a bit higher for motion (than appearance/disappearance) because there is simply more to observe. All had the same exclusion errors, GeoLocate had more intrusion errors. From the observation of participants, GeoLocate seemed to be used incorrectly. The prototype was designed such that the information about moving towards would be accessed by swiping the screen *after* viewing the notification list.

However, many participants did not engage in that step, and tried to assess motion from the notification list. GeoWatch had more intrusion errors than GeoBar. The reason may be the fact that GeoWatch provides another feature that is similar to the moving toward, and the two may be confuseable. For the identification of location viewers moving away, GeoLocate and GeoBar were not different (about 59%). These prototypes differed on intrusion errors (GeoWatch higher than GeoBar). This is likely caused by the fact that GeoBar has the feature of moving away while GeoWatch has the feature of moving away and moving toward then away. Participants in GeoWatch may have mixed the features. Technically, only GeoWatch offers the feature of moving toward then away, but GeoBar offers moving toward and moving away so some participants may have mixed the features or tried to combine the features to create an answer.

The final tasks asked participants to find the distance to particular location viewers: “How far is “Person X” from your location?” and “How far is “Person Y” from your location?” This required first finding the viewer, and then the distance. Some of the location viewers were themselves in motion. Performance was high and similar for all prototypes (about 90%). This task does not delineate prototypes despite the different interfaces.

Generally, in terms of performance, all prototypes were successful. The differences between prototypes seemed minor. It must be remembered that three *viable* prototypes were designed. None was intended as a bad or pointless prototype. As such, it is reasonable to expect that each would have some good and bad features. GeoLocate was the easiest to use for finding the number of viewers, identification of viewers, and the distances to viewers.

The rank order of performance indicated that GeoLocate was the highest (Table 4.20), but it did not offer the same number of features as GeoWatch or GeoBar. Hence, ratings need to consider that. In the real world, some features might be more important than others (this is why affect ratings are necessary), and the lack of a particular feature could render a prototype “useless” to users.

Previously noted that 85.7% of respondents indicated that they would install the app that has this feature (Prototype), and 47.6% would use it. From this, we can see that participants liked the idea of an awareness mechanism, and that about half use it. This implies that about half of the participants see usability problems (e.g., font or size of icons) or that the information is not something that they would care to know. Usability issues are to be expected: This study is the first stage of design, and the prototypes were not fully functioning apps. Further designs would

combine the better element of all three prototypes.

In addition, results showed that 42.9% of respondents would want to be notified about viewers who are in their city, while 52.9% would want to be notified about viewers from any location in the World. Although participants had a slight (non-significant) preference for feedback about viewers the world over, they may not have realized that doing so would more intrusive (use more of the screen), be harder to read, and make it harder to find the important information (e.g., who is near; particular individuals). For example, restricting the list to only those in one's city would be more useful if worried about stalkers.

A number of affect measures were collected about each prototype (Tables 4.21 and 4.22). Generally, in terms of overall ratings, the prototypes were easy to use, understandable, enjoyable and aesthetically pleasing. However, GeoLocate was rated lower on the usefulness of the provided information (which may reflect its inability to perform some tasks) and on the ability to continue broadcasting while checking viewers. GeoLocate requires more attention to parse the information. Generally, it could be said that GeoBar would be the least intrusive while broadcasting: The radar plot in GeoWatch obscures the screen and the list in GeoLocate partially obscures the screen.

#### **4.5.4 Design Implications for Location Viewers Feedback**

In addition to the design guidelines that we used to design the Feedback Mechanisms (Section 4.1.1) we list other design implications based on our results of the two awareness mechanisms.

- **Design Attention:** Salience is the first component of design awareness. Our results showed that a continuous growing and shrinking icon (a dynamic icon) was the best to be noticed for identifying the number of viewers, comparing to the other designs (Section 4.4.3.1).
- **Design for accommodation:** Making the design to accommodate large number of viewers (e.g., GeoWatch shows a radar that can represent large number of viewers). This guideline is also consistent with Jedrzejczyk (2012).

- **Design for less intrusiveness:** Having a smaller number of features (the most important or the most risky features) to notify could be a solution for intrusiveness (e.g., showing viewers only from the broadcaster’s city, or warning the broadcasters only about viewers who could pose a risk e.g., viewers just checked the location, closest viewers, and viewers who are moving toward the location. This is consistent also with Zhou (2015) notification design guidelines. In addition, design a visual representation that makes the user to see the viewers at once without the need to navigate or interact with the design to know more about specific viewers, which implied another design implication is design for less effort use. Participants’ respondents on GeoBar show that. One respondent reported: “*i [sic] can view the infor [sic] without any interruption of the broadcast*”, another: “*less distracting compared to other two applications*”, another: “*It shows me the user distances even without interacting with it and still keep broadcasting.*” another participant: “*Easy to interact while broadcasting*”, another respondent said: “*I can see my viewer's locations and also my broadcast at the same time.*” another one: “*gives me a visual sense of who is closer to my location without an effort of displaying their information*”.
- **Design for the appropriate position:** One of the important design implications for the context of live video broadcasting is not to make the feedback design obscure the view of the broadcast, so that the broadcaster can see themselves while broadcasting. We found that the best representation of feedback is to be placed at the top of the screen. One respondent said “*i [Sic] like here was that i [Sic] can see list of people all above and easier i [Sic] can see their distance*”, another one reported “*The icons were easy to see and access It doesn't interfere with the broadcast yet, shows user location in interaction way.*”
- **Design an effective representation of the viewers:** Provides direct viewers’ identities representation (e.g., profile photo for easy face recognition/non-recognition) instead of using circle/dots objects that requires clicking on to see the viewer. A respondent said: “*It is very easy for me to know who is exactly closer to my location without even clicking on*” another one: “*The information about the viewer. I can visually recognize who is closer to my location*”



- **Design an explicit and dynamic representation to show proximity:** Use color-coding aiming to show the level of risk and/or dynamic objects that visually represent proximity of the viewers. One participant reported: *“It as [Sic] super easy to use to get notification about who is near my approximate distance.”* another one: *“very easy to see the most near by individuals”*
- **Intend for enjoyable design:** Avoid the standard way of designing (i.e., a list to show viewers) and make the design enjoyable or creative but simple to deliver the message. This would make people use it and check viewers around them regularly so that they have a better sense of viewers around them. One respondent reported: *“it was enjoyable for me to know which 2 people are at the same position”*, another one: *“Graphical representation, easier to understand, fun to use”*, another respondent commented on GeoLocate: *“not interactive and fun as other apps”*

#### 4.5.5 Comparisons of Visual Privacy Awareness Prototypes

In this section we compare the three prototypes of Visual Privacy Awareness.

The Visual Privacy Awareness prototypes were tested in a more general way because the main goal is to examine the acceptance of the idea. There were no specific tasks to perform. Participants simply worked with each (in a counterbalanced order) and then provided ratings on a number of dimensions (Tables 4.26 and 4.27). Ratings were generally favorable on ease of performance, understandability, aesthetics, enhancing security, enhancing behavioral awareness (2 items). All prototypes were the same with a mean above 4 on a 5-point scale. All prototypes were rated high for ease of use and understandability when in a good mood (mean ratings above 4). In general, all these items (particularly security and behavioral awareness) confirm that this feature/concept could be important in the context of live video broadcasting.

However, ratings for ease of use and understandability when in a bad mood, and ratings for ease of use and understandability when intoxicated were much lower (less than 4) and dipped as low as 2.4 (3 would be neutral). This is important because these are the questions that relate to the use of this type of app when this app would be most useful (i.e., when privacy might be compromised by mood or by mood altering stimulants). As such, the differences between the

prototypes becomes important. Note that for Questions that ask about understandability and ease of use when intoxicated, Mood-to-Mood is different (lower than) from Appearance-to-Mood and Mood-to-Mood is different (lower than) from Appearance-Directly, but Appearance-to-Mood and Appearance-Directly are the same. Hence, the overall conclusion would be to avoid Mood-to-Mood. The choice of Appearance-to-Mood or Appearance-Directly would be fine. In some sense, the lower ratings on these items is exactly the intent of the prototypes. If performance falls, then the prototypes would default to a mode that protects the privacy of the broadcaster. Ratings were also lower for enjoyment (below 4). The three prototypes also differed on the intoxicated items. For intoxication, Mood-to-Mood was the lowest on ease of use and understandability — significantly lower than Appearance-to-Mood and Appearance-Directly. From a privacy perspective, this means Mood-to-Mood would be more secure and more likely to invoke privacy measures.

From the previous analysis of rating as a function of the three prototypes (Table 4.27), we can see that while the choice of prototype would be based, to some degree, on personal preferences, Mood-to-Mood has a lower overall rating, and a higher standard deviation. It also has the lowest maximum. Hence, it is not likely the best choice.

However, ease of use does raise the question of whether or not the prototypes would be used at all. Many of participants (57.1%) indicated that they would install it, 47.6% would use such features, and 42.9% indicated they prefer blurring for protecting the visual privacy of others. In general, although 47.6% of respondents would like to use this type of app, across all measures Prototype Appearance-Directly received the highest ratings and it is the most likely to be effective. This indicates participants like the concept, but probably further design improvement needed to obtain higher acceptance of the technology.

#### **4.5.6 Design Implications for Visual privacy Awareness**

In addition to DwI design guidelines that we used to design our Visual privacy mechanism (Section 4.2.1), our results emphasize some design aspects for the context of live video broadcasting as following:

- **Simplicity:** Design an easy interface to test the state of mind that is easy for self-aware people and a little difficult for unthinking people. A participant commented on Appearance Directly task: “The choice is clear and the reason is clear” another one reported: “the mood question does help me reconsider my actions”
- **Context-awareness to preserve privacy:** Include more context information, such as different mood states, inappropriate behavior, types of audience (viewers) (e.g., family, friends, strangers, etc.), and people surrounding) to notify the user and protect his privacy. A respondent reported on Appearance-to-mood task: “predicts the mood of the people by choosing the right or wrong face.”, and another one : “It protects me from presenting bad behaviour” another participants said: “Automatically selecting filter is a great idea as sometime you forget to select filter but selecting mood can save you in some place.” Also another one reported: “Great idea for when you're drunk or angry and not making good choices in social media”
- **Flexibility:** provide different visual tasks for positive and negative mood, and the flexibility of a system to enable the user to opt out/in. A respondent said: “I can chose were to put my real face and make people know my real identity which is my major concern while broadcasting.”
- **Design for influencing behavior: this can be achieved by:**
  - **Transparency:** providing a direct preview of what the broadcast would be before applying the visual privacy protection, and also to make him aware of his visual appearance. A respondent reported: “*It shows me what kind of category I will present my face*” another one: “*it remind me of the type of audience that might be seeing my broadcast.*” Another participant said: “*helps to control my emotions and behavior*”
  - **Reminder:** remind the user about the expected audience so that the broadcaster may reconsider his/her behavior. This reminder can inform the broadcaster’s decision and affect his/her behavior. One participant reported: “*It gives a subtle reminder of who may be watching me and what the consequences that it can have.*” Another one said: “*Safety filter protects our identity from false hands.*” Another respondents reported: “*Automatically selecting filter is a great idea as*

*sometime you forget to select filter but selecting mood can save you in some place.”*

## **4.6 Limitations**

In this section we describe the limitations for the Location Viewers Feedback and Visual Privacy Awareness experiments.

### **4.6.1 Location Viewers Feedback Experiment**

The current study provides a reasonable first-round of prototype design and testing. The results suggest that all prototypes had some good features and some not-so-good features. As noted previously, all were designed as viable option so this is not surprising. Nonetheless, the ultimate goal would be a single useful design that is easy to use and useful. To achieve this goal, several steps can be taken.

Firstly, it must be acknowledged that temporal live video broadcasting apps are recently developed, and the current prototypes offer new functionality on top of a new app. As such, potential users may not yet truly know what they would want from such apps. They may not yet know what the location prototypes would be used for in the real world. Participants did indicate some interest in installing and using these prototypes, but the exact use is not yet known. For example, is a broadcaster ever going to want a list of all the people who viewed the broadcaster’s location? Is it more likely that they want to know who is close or who is approaching? We tested both, but both might not be of equal value. Another issue is the number of location viewers. How many viewers will actually check locations? The current prototypes present 8 location viewers. However, if there are 1000 or more, some other approach (some filtering) will be needed. Although we proposed the designs based on showing viewers who are in the same city of the broadcaster, more realistic experiment (e.g., Wizard of Oz) is needed to examine how successful this feature would be.

Hence, more testing is warranted. In particular, we need to know how the prototypes would be used in the real world. What features would dominate? More testing is required for

more mundane reasons as well.

Another limitation problem is that it would be more effective if we could have the same survey participants to participate in the experiment to see the link between the survey responses, and the experiment results. However, that was difficult because the survey participants were international.

At times, it seemed that participants were overwhelmed by the task requirements, and therefore sometimes not accurately answering the questions. Whether this is a problem with the software used for designing the prototype or a problem with the experimental procedure (e.g., the amount of time for familiarization, the wording of questions, the order of tasks). The software that we used to implement our prototypes, sometimes, it did not quickly comply with clicking on objects. So, we were expecting usability problems because of the software we used to design our prototypes.

Another problem we encountered was that although participants were asked for replaying the prototype before answering each question if needed, most did not replay it. So they were answering questions based on last moments of a moving feature, which affect the accuracy of the answers.

One can note that performance seems to be higher with the later questions. This may reflect familiarity with the prototypes. The prototypes were tested in a pre-programmed manner. This allowed for experimental control but is not particularly realistic. Participants could not “play” in a general sense to gain familiarity.

Moreover, Participants had knowledge in advance about what the study is about, which might affect some participants when they answer our questionnaire. Our experiment was performed with small size of participants, making the findings hard to be generalized.

#### **4.6.2 Visual Privacy Awareness Experiment**

The main question that one would have about this feature (these prototypes) is actual use. They are designed to protect broadcasters when the ability of broadcasters to protect themselves is compromised. That implies an extra step before each use — an extra step that might just annoy some users. This needs to be tested. There is always a trade off between usability and security.

This feature would be better for drunken people, but maybe not for those who are simply sad, angry. However, not having participants in the state of negative moods (e.g., depressed) or under the influence of alcohol, would not measure the accuracy of our proposal visual privacy awareness designs. In fact, having those participants are restricted from ethics board due to their sensitive situations. However, if we could have those participants, Wizard of Oz is the best to test the effectiveness of the prototype (Usability Net, n.d.). Therefore, this study is an early stage of design that we wanted to examine whether users, who have privacy concerns, would accept this technology in the context of live video broadcasting, and whether the interface help addressing the visual privacy issues, so that the experiment and designs can be developed in the future to better set up for accuracy results.

The third prototype seems to have the most favorable ratings (Appearance-Directly), but the third prototype does not really impose any security. It simply reminds people to do so. As such, it might not be too useful when it is most needed. The problem with intoxication (or extreme moods) is that they impair cognition (that is why it is called “impaired driving”). Hence, the user might not have sufficient presence of mind to impose controls.

## **4.7 Future Work**

This work focused on the privacy awareness as a solution for privacy issues associated with live video broadcasting apps. The work can be developed for the future in the following aspects:

### **4.7.1 Location Viewers Feedback Prototypes**

- One suggestion would be the development and test of a single prototype that combines the best features of all three. For example, the general layout of GeoBar could be combined with a radar plot (on demand) or a list (on demand).
- Some possible improvements that should be considered on the designs are icons size, affording high number of viewers.
- Considering participants’ suggestions to improve the designs (see Section 4.4.3.1.2).

- Applying GeoBar prototype, one design challenge that can be encountered is how to show a group of viewers located at the same location, in a small space of screen, and while broadcasting. Using a network of circles might help partially to solve the problem. More investigation needed.
- Additional information to be added on the feedback e.g., direction of viewers, whether the viewer is a follower on a broadcaster's contact list, a family member(s), a friend(s), or a stranger.
- A challenge that needs to be considered is how to make the design to differentiate between BCs' viewers and location viewers (Viewers who are watching the broadcasts, but not necessarily the broadcaster's location), and location viewers (who are watching the broadcast and the broadcaster's location) for the apps that provide both features. Specifically, how to make the design accommodate these two features, on small-size display screens.
- Another possible investigation related to location viewers is, whether the viewers would stop checking the location if he/she knows that the broadcaster is aware of movement of the people around him?
- The need for location viewers aggregated list so that the user can check it anytime to see who viewed his location.
- Changing the setting of the location viewers experiment into Wizard of Oz experiment to obtain better sense of the effects and results of the proposed work due to observing participants' actual behavior. Meaning that the work should be programmed with real live video broadcasting, providing the awareness mechanisms while broadcasting to examine awareness (attention), distraction and reaction.

#### **4.7.2 Visual Privacy Awareness Prototypes**

In this section we highlight some of the future work that we would like to implement if we had the time to develop such prototypes.

- Changing the setting of the visual awareness experiment into programming live video broadcasting app with the proposed awareness mechanism, supplied with a video camera

recorder, and screen recorder. The recruitment would be for broadcasters who using live video broadcasting for seeking emotional support, for self-expression, or those who use it when they are in negative moods. Therefore, we can obtain better insight about the usefulness and ease of use of the proposed design, and the actual reaction of broadcasters.

- Another possible development of experiment is Sentiment analysis of the translated video broadcast, transfer the videos into text to examine the actual mood of the broadcaster.
- Another possible improvement, beside the mood, is to classify the audience/viewers into family, friends, strangers or broadcasting simultaneously to people who will see your explicit appearance (selected by the broadcaster) and people who will not see the appearance (selected by the broadcaster).
- Another improvement that can be performed is when the system detected that the broadcaster should be blurred, it automatically blocks the contact/followers list, so that people who are in the broadcaster's list do not know that he is in that negative/atypical mood. At the same time if the broadcaster was broadcasting publicly, he will be presented in blurring filter with blurred profile image. Also, the blurred broadcasts will be self-destructing, means that a blurred broadcast will be deleted immediately once the broadcaster end his broadcast. The purpose of these features is to reduce the possibility of the broadcaster to be self-disclosure in the negative moods. Only explicit broadcasts will be lived up to 24 hours, others blurring broadcasts would be immediately deleted after the broadcast ends.
- Another set of prototypes might be designed that automatically blur (or hide). The user would then have to "pass some tests" to lift that blurring. For example, a simple test of intoxication would be to place a moving dot on the screen. The user would have to hit the dot to avoid blurring the image. Hand to eye coordination is impaired by most stimulants. The speed of the dots/circles movements, which represent the movement of viewers, (and the randomness of the motion) could be varied. Pressure sensitive screens might be useful for anger.
- Participants' suggestions are very useful, and can be implemented for further design exploration (Section 4.4.3.2.2)



## CHAPTER 5 CONCLUSION

Temporal, self-destructing (“ephemeral”) live video broadcasts (BCs) are a recent tool for social media. Live-Video Broadcasting apps (LVB apps) such as Periscope, YouNow, or Meerkat provide new easily used tools for live broadcasting, but these raise unique privacy concerns for several reasons.

Firstly, many BCs are informal and spontaneous (unplanned) making certain aspects of self-moderation difficult. It seems likely there is a tendency to increased self-disclosure in such settings and also a tendency to overlook issues of privacy. Many LVBs are public which increases issues of privacy.

Secondly, the temporal nature may lead to different patterns of usage, or different beliefs about privacy. For example, while broadcasters cited many concerns they also have a tendency to overrate the privacy afforded by the temporary nature of the BC (e.g., other apps are designed to capture such BCs), and patterns of use are still evolving. For example, Periscope offers temporary storage of BC for up to 24 hours and broadcasters see some merit in that. Hence, to compete, other apps will likely offer similar services.

Thirdly, public BCs are, largely, an unknown territory, particularly the public BCs of a personal nature that reveal details about home and location. Experience of the Internet has clearly demonstrated that there are numerous malicious individuals who will take advantage of others. Public BCs on a global scale create more opportunities for such malice.

As such, LVBs require special attention in order to preserve user privacy. We investigated usage patterns and privacy concerns through online survey. Results showed that BCs are used for a mix of formal and informal reasons: BCs are used for a mix of videos of self and others, many BC are public, most BC are made while happy, but substantial numbers are made while worried or angry. Ephemeral BCs are used to provide privacy, and users want more control over various aspects of the BCs. In our second study, we explored three real-time feedback designs to provide the broadcaster with feedback about viewers — particularly viewers who checked the broadcaster’s location. We also explored three mood-based visual privacy

settings designed to protect a broadcaster from their own behavior that would be inappropriate while broadcasting.

## 5.1 Study 1 and Study 2

The two studies conducted in this work were quite different and yet related. The first study was a survey of current usage and concerns (particularly about privacy and security). One result indicated that the lack of knowledge about who had viewed their location was the highest concern (rated 2.15 out of 3). This was related to a fear of physical harm (rated 2.02 out of 3; the second highest concern). In addition, 67% of broadcasters indicated that GPS location is something that LVB apps should keep private (the highest endorsement). Most broadcasters (81% of respondents) also indicated that they would like feedback about who had viewed their location (this was highest endorsement for feedback). Another result indicated that broadcasters are concerned about social reputation (rated 2.01 out of 3; the third highest concern, and a substantial minority (45%) considered “my inappropriate behavior” to be something that LVB apps should keep private (the second highest endorsement).

The second study designed, developed and experimentally tested three prototypes for providing broadcasters with feedback about who viewed their location. While the design of the prototypes predated the survey results, it was based on similar comments in the literature.

In the second study, a second set of three prototypes were designed, developed and experimentally tested for mood-based privacy awareness mechanisms. It is difficult to define “inappropriate behavior” because it could be many things to many people, and it could be different things to different people. However, inappropriate behavior is associated with negative moods (e.g., anger, depression) and with the used of stimulants such as alcohol (see for example, Dayan & Huys, 2008, Kopelman, 2001). Hence the app was designed to remind broadcasters of the implications of broadcasting while in a negative mood. Two of the three apps provided default privacy protection if the broadcaster should indicate a negative. mood.

Hence, the two studies were linked in that the prototypes (which provide add on features for LVB apps) were designed to provide the most requested privacy features. The location prototypes could be considered successful. After working with the prototypes 86% said they

would install such features, while 48% said they would use it regularly. The privacy prototypes were less successful in that after working with the prototypes only 57% said they would install such apps, while only 47% said they would use it regularly.

The two studies based inferences on the same general population of broadcasters (not viewers). However, the survey was based on an international sample while the experiments were necessarily based on a local sample. However, a comparison of demographics indicated that both studies had a mix of genders (i.e., the first was 56% female while the second was 24% female) and overlapping ranges for age and educational backgrounds (the international survey was more diverse). They had overlapping self-reported comfort with technology and overlapping self-reported knowledge of security, though the experimental study was higher on both (it was drawn from a faculty of computer science). More important, the pattern of use collected in the experimental study (apps used, reasons for use, categories of use, audience type, planning, and location) mirrored the pattern of use collected in the larger survey, and the cited concerns were the same (i.e., GPS location and inappropriate behavior were the highest cited for sensitive information; mood was a factor for inappropriate behavior). As such, we can be reasonably sure that the results for the experimental study would apply more broadly within the international community of broadcasters.

## **5.2 Thesis Contribution**

The survey contributes a wealth of descriptive statistics about the use of live video broadcasting apps and the associated issues for privacy (and security). Such data is lacking, and the lack is an impediment to further research on the emerging role of such apps in social media. The insights gained from the survey would also be useful for helping to understand how (or what) to teach broadcasters about privacy when using live video apps. It provides valuable information about what level of control and ease of use that broadcaster would want or expect

Generally, it seems that broadcasters would like to have information about viewers who examined their location displayed in a non-intrusive fashion (does not obscure the BC) that also provides information about the movement of location viewers. The third prototype seemed the most preferred, but it would likely benefit from the inclusion of features from the other two. This

work contributes to the ongoing development of privacy enhanced social media apps. It shows that privacy can be incorporated as a part of design, and that potential users could enjoy the feature. Furthermore, the features developed herein could be applied (in principle at least) to any location-sharing app.

Furthermore, the visual privacy awareness mechanisms prototypes contribute in several ways. They provide and test a model that places a mood self-assessment task before broadcasting. This task reminds the broadcaster about the obligations to self. The results indicated that the approach would likely work. Therefore, this work contributes in highlighting the importance of visual privacy protection in the context of live video broadcasting. It also suggests and informs designer about methods to test the user whether they under the influence of alcohol. It evaluates how the user would accept this technology in live video broadcasting. It also provides an opportunity to those who intend to use live video broadcasting for personal reasons, and want to preserve their social or professional reputation. Overall, it can decrease the level of self-disclosure behavior in the sense that their visual is protected. For all proposed designs, they can improve perceived awareness and privacy, and they might also contribute to the design of third-party apps to improve privacy. Although many seem to accept that feature, the percentage might be not significantly high. As such, the current work contributes one possible mechanism but leaves open the possibility that there may be better ways.

### **5.3 Limitations**

The specific limitations of each study have been discussed along with each associated study. However, some bear repetition and there are some general limitations that apply more broadly.

Firstly, for both studies, the sample size was limited. This was particularly true for the survey. The knowledge extracted from a questionnaire is limited by the design of questions (items). In case there was little prior research to guide the design of items so some aspect that would have been interesting were not explored (e.g., which methods would be used for which concerns). The survey was likely too long, affecting response rates.

Secondly, the location prototypes were not functional prototypes. The participants interacted with a pre-programmed user interface and responded to questions in a linear fashion.

This is not representative of the real world. In particular, it is not representative of the cognitive load associated with checking location information *while* broadcasting. It is also not representative of the manner in which users would interact with the GUI. In addition, participants had little exposure to the actual prototypes, and little time to consider the implications of the features proposed (tasks used). Hence, their performance may not be reflective of long term use.

Thirdly, the visual privacy awareness prototypes share some of the same concerns. The prototypes were not functional. The participants interacted with a pre-programmed user interface and responded to questions in a linear fashion, which is not likely how they would be used in the real world. In particular, the experimental situations is not representative of the use of such prototypes when needed: that is, when the user is in a negative mood — particularly an extreme negative mood — or under the influence of stimulants.

## 5.4 Future Work

Specific recommendations for future work were discussed previously along with each associated study. However, some bear repetition and there are some general recommendations that apply more broadly. In addition, future work is the natural extension of limitations.

Firstly, for both studies, the sample size was limited. This was particularly true for the survey. However, before sampling more broadly, the survey should be refined, based on the responses obtained. That is the survey should be shortened, simplified and refocused in light of responses.

Secondly, the location prototypes could be refined — and possibly a single prototype that combines the best feature of all could be developed and tested. This second round of testing should use functional prototypes that allow the users to have more control over the interactions with the GUI. In particular, it would be useful to see how the prototype functions *while* broadcasting. While broadcasting, the user must split attention between the broadcast itself and the feedback provided. That might lead to further design considerations. There are numerous other “minor” changes that could improve the experience (e.g., font sizes and colors, icon size and colors, data presentation modes, filtering of information particularly when there is too much, integration with other features offered in these apps). It also contributes in informing what design

is most preferred by users, and can be improved and used for live video broadcasting.

Thirdly, we think that new Visual Privacy Awareness prototypes need to be developed. In the current work, the prototype most preferred by users was one that simply “reminded” broadcasters of their obligation to themselves and others. It did not provide any test of mood; it did not impose or default to any standard of privacy. As such, one can easily imagine that it would be of little use when the broadcaster was in a negative mood (e.g., angry, frustrated, depressed) or under the influence of stimulants. As with Location Viewers Feedback prototypes, it would also be useful to have functional prototypes so to see how the designs would function in the real world. In particular, the prototypes should protect users when in negative moods. Unfortunately, inducing strong negative moods is almost impossible in an experimental setting (ethical issues are another consideration) so such would have to field tests.

Additional prototypes can be developed that provide other types of protection. That is, the survey identified other concerns, and no doubts that future surveys (and real world use) will uncover still further concerns. Hence, prototypes will need to be developing to provide these features. It would be most useful if any new features tried to use a common interface — at least, as common as possible.

Questions of how concerns about privacy vary by culture are complex. The survey and prototypes must be refined to reflect cultural values. This might be particularly true of the privacy prototypes (e.g., issues of alcohol consumption cross-culturally). The current work attempted to be inclusive, but cultural issues were not a design focus.

## BIBLIOGRAPHY

- [1] AAA DUI Justice Link. (n. d.). *Standardized Field Sobriety Test*. Retrieved from <http://duijusticelink.aaa.com/issues/detection/standard-field-sobriety-test-sfst-and-admissibility>
- [2] Abraham, A. R., Prabhavathy, A. K., & Shree, J. D. (2012). A survey on video inpainting. *International Journal of Computer Applications*, 56(9).
- [3] Ackerman, M. S., & Mainwaring, S. D. (2005). Privacy issues and human-computer interaction. *Computer*, 27(5), 19-26.
- [4] Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy*, (6), 82-85.
- [5] Acquisti, A. (2012). Nudging privacy: The behavioral economics of personal information. *Digital Enlightenment Yearbook 2012*, 193-197.
- [6] Acquisti, A., & Grossklags, J. (2003, May). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *2nd Annual Workshop on Economics and Information Security-WEIS* (Vol. 3, pp. 1-27).
- [7] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514.
- [8] Adams, A., & Sasse, M. A. (2001). Privacy in multimedia communications: Protecting users, not just data. In *People and Computers XV—Interaction without Frontiers* (pp. 49-64). Springer London.
- [9] Agrawal, P., & Narayanan, P. J. (2011). Person de-identification in videos. *IEEE Transactions on Circuits and Systems for Video Technology*, 21(3), 299-310.
- [10] Albrecht, K., & McIntyre, L. (2015). Psst... Your Location Is Showing!: Metadata in digital photos and posts could be revealing more than you realize. *IEEE Consumer Electronics Magazine*, 1(4), 94-96.

- [11] All Things Digital. (2013). *YouNow Gives Stage to Internet's Wannabe Stars, Leaves Judgment in Your Hands*. Retrieved from <http://allthingsd.com/20130212/younow-gives-stage-to-internets-wannabe-stars-leaves-judgment-in-your-hands/>
- [12] Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. & Agarwal, Y. (2015, April). Your Location has been Shared 5,398 Times!: A Field Study on Mobile App Privacy Nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 787-796). ACM.
- [13] AlSagri, H. S., & AlAboodi, S. S. (2015, June). Privacy awareness of online social networking in Saudi Arabia. In *Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2015 International Conference on* (pp. 1-6). IEEE.
- [14] Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*.
- [15] Amichai-Hamburger, Y., Wainapel, G., & Fox, S. (2002). " On the Internet no one knows I'm an introvert": Extroversion, neuroticism, and Internet interaction. *CyberPsychology & Behavior*, 5(2), 125-128.
- [16] Anthony, D., Henderson, T., & Kotz, D. (2007). Privacy in location-aware computing environments. *IEEE Pervasive Computing*, (4), 64-72.
- [17] Archer, T. M. (2007). Characteristics associated with increasing the response rates of web-based surveys. *Practical Assessment Research & Evaluation*, 12(12).
- [18] Archer, T. M. (2008). Response rates to expect from web-based surveys and what to do about it. *Journal of Extension*, 46(3), 3RIB3.
- [19] Balebako, R., Leon, P. G., Almuhimedi, H., Kelley, P. G., Mughan, J., Acquisti, A., Cranor, L. & Sadeh, N. (2011, May). Nudging users towards privacy on mobile devices. In *Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion*.
- [20] Beldad, A., & Kusumadewi, M. C. (2015). Here's my location, for your information: The impact of trust, benefits, and social influence on location sharing application use among Indonesian university students. *Computers in human behavior*, 49, 102-110.
- [21] Bellotti, V., & Sellen, A. (1993). Design for privacy in ubiquitous computing environments. In *Proceedings of the Third European Conference on Computer-Supported*



*Cooperative Work 13–17 September 1993, Milan, Italy ECSCW'93* (pp. 77-92). Springer Netherlands.

- [22] Benisch, M., Kelley, P. G., Sadeh, N., Sandholm, T., Cranor, L. F., Drielsma, P. H., & Tsai, J. (2008). *The impact of expressiveness on the effectiveness of privacy mechanisms for location sharing* (No. CMU-ISR-08-141R). CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE.
- [23] Biocca, F., Harms, C., & Burgoon, J. K. (2003). Toward a more robust theory and measure of social presence: Review and suggested criteria. *Presence*, 12(5), 456-480.
- [24] Boyle, M., Neustaedter, C., & Greenberg, S. (2009). Privacy factors in video-based media spaces. In *Media Space 20+ Years of Mediated Life* (pp. 97-122). Springer London.
- [25] Buhler, T., Neustaedter, C., & Hillman, S. (2013, February). How and why teenagers use video chat. In *Proceedings of the 2013 conference on Computer supported cooperative work* (pp. 759-768). ACM.
- [26] Chen, G. M. (1992). Differences in self-disclosure patterns among Americans versus Chinese: A comparative study.
- [27] Cho, S. H. (2007). Effects of motivations and gender on adolescents' self-disclosure in online chatting. *CyberPsychology & Behavior*, 10(3), 339-345.
- [28] CNNMoney. (2015). *Meerkat Who? Introducing Periscope*. Retrieved from <http://money.cnn.com/2015/03/26/technology/periscope-livestream-twitter/>
- [29] Cohen, J. (1988) *Statistical Power Analysis for the Behavior Sciences*. (2nd Ed). New York: Academic Press.
- [30] Conti, G., & Sobiesk, E. (2010, April). Malicious interface design: exploiting the user. In *Proceedings of the 19th international conference on World wide web* (pp. 271-280). ACM.
- [31] Correa, T., Hinsley, A. W., & De Zuniga, H. G. (2010). Who interacts on the Web?: The intersection of users' personality and social media use. *Computers in Human Behavior*, 26(2), 247-253.

- [32] Courtois, C., Mechant, P., Ostyn, V., & De Marez, L. (2013). Uploaders' definition of the networked public on YouTube and their feedback preferences: a multi-method approach. *Behaviour & Information Technology*, 32(6), 612-624.
- [33] Cranor, L. F. (2014). Conceptions of Privacy.
- [34] Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science*, 10(1), 104-115.
- [35] Dailymail. (2010). *The Social Media Sobriety Test: New web app stops you posting on Facebook and Twitter if you're too drunk*. Retrieved from <http://www.dailymail.co.uk/sciencetech/article-1328739/Facebook-gets-Social-Media-Sobriety-Test-check-youre-drunk-post.html>
- [36] Dextro. (2015). *Online Video Discovery*. Retrived from <https://www.dextro.co/discovery>
- [37] Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- [38] Ding, Y., Du, Y., Hu, Y., Liu, Z., Wang, L., Ross, K., & Ghose, A. (2011, November). Broadcast yourself: understanding YouTube uploaders. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 361-370). ACM.
- [39] Duckham, M., & Kulik, L. (2006). Location privacy and location-aware computing. *Dynamic & mobile GIS: investigating change in space and time*, 3, 35-51.
- [40] Dumais, J. (2015, April 24). *Live video broadcasting apps Meetkat, periscope, and YouNow - okay for kids?*. Retrieved September 5, 2015 from <http://www.bewebsmart.com/app-review/meerkat-periscope-younow-okay-for-kids/>
- [41] Edworthy, J. (Ed.). (1996). *Warning design: A research prospective*. CRC Press.
- [42] Ehrenberg, A., Juckes, S., White, K. M., & Walsh, S. P. (2008). Personality and self-esteem as predictors of young people's technology use. *Cyberpsychology & behavior*, 11(6), 739-741.

- [43] Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook “friends:” Social capital and college students’ use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143-1168.
- [44] Flynn, K. (2016, January 19). Shorty Awards 2016 Nominees Brings Periscope, YouNow Stars Legitimacy In Media Industry. *International Business Times*. Retrieved from <http://www.ibtimes.com>
- [45] Ford, D. (2015, October, 13). Women live streams herself while driving drunk, police say. *CNN*. Retrieved from <http://www.cnn.com>
- [46] Frome, A., Cheung, G., Abdulkader, A., Zennaro, M., Wu, B., Bissacco, A., Adam, H., Neven, H. & Vincent, L. (2009, September). Large-scale privacy protection in google street view. In *2009 IEEE 12th international conference on computer vision*(pp. 2373-2380). IEEE.
- [47] Gaver, W. W. (1991). Sound support for collaboration. In *Proceedings of the Second European Conference on Computer-Supported Cooperative Work ECSCW'91* (pp. 293-308). Springer Netherlands.
- [48] Gedik, B., & Liu, L. (2005, June). Location privacy in mobile systems: A personalized anonymization model. In *Distributed Computing Systems, 2005. ICDCS 2005. Proceedings. 25th IEEE International Conference on* (pp. 620-629). IEEE.
- [49] Geier, B. (2015, March 9). Everything you need to know about the hot news app Meerkat. *Fortune*. Retrieved from <http://fortune.com>
- [50] Goessl, L. (2012). New japanese security camera scans 36 million faces per second. Retrieved from <http://digitaljournal.com/article/321848>
- [51] Goh, J. M. (2011). *The cultural self: experiments investigating self-awareness and self-disclosure in computer-mediated communication* (Doctoral dissertation, University of Manchester).
- [52] Günther, J. (2007). *Digital natives & digital immigrants*. Innsbruck: Studienverlag.
- [53] Hachman, M. (2015, March 13). Twitter buys Periscope as its livestreaming response to Meerkat. *PCWorld FROM IDG*. Retrieved from <http://www.pcworld.com>

- [54] Hamburger, Y. A., & Ben-Artzi, E. (2000). The relationship between extraversion and neuroticism and the different uses of the Internet. *Computers in Human Behavior*, 16(4), 441-449.
- [55] Hansen, M. (2009). Putting Privacy Pictograms into Practice-a European Perspective. *GI Jahrestagung*, 154, 1-703.
- [56] Hartsell, T., & Yuen, S. C. Y. (2006). Video streaming in online learning. *AACE Journal*, 14(1), 31-43.
- [57] Holtz, L. E., Nocun, K., & Hansen, M. (2010). Towards displaying privacy information with icons. In *Privacy and Identity Management for Life* (pp. 338-348). Springer Berlin Heidelberg.
- [58] Hong, J. I., & Landay, J. A. (2004, June). An architecture for privacy-sensitive ubiquitous computing. In *Proceedings of the 2nd international conference on Mobile systems, applications, and services* (pp. 177-189). ACM.
- [59] Howell, D.C (1997). *Statistical Methods for Psychology*. (4th Ed). Belmont, CA: Duxbury Press.
- [60] Jarvey, N. (2015, October 13). Live-Streaming Startup YouNow Taps Fullscreen Veteran (Exclusive). *The Hollywood Reporter*. Retrieved from <http://www.hollywoodreporter.com/>
- [61] Jedrzejczyk, L. (2012). *Supporting Location Privacy Management through Feedback and Control* (Doctoral dissertation, The Open University).
- [62] Jedrzejczyk, L., Price, B. A., Bandara, A. K., & Nuseibeh, B. (2010, July). On the impact of real-time feedback on users' behaviour in mobile location-sharing applications. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 14). ACM.
- [63] Jensen, C., & Potts, C. (2004, April). Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (pp. 471-478). ACM.

- [64] Joinson, A. (1999). Social desirability, anonymity, and Internet-based questionnaires. *Behavior Research Methods, Instruments, & Computers*, 31(3), 433-438.
- [65] Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. *European journal of social psychology*, 31(2), 177-192.
- [66] Judge, T. K., & Neustaedter, C. (2010, April). Sharing conversation and sharing life: video conferencing in the home. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 655-658). ACM.
- [67] Juhlin, O., Engström, A., & Reponen, E. (2010, September). Mobile broadcasting: the whats and hows of live video as a social medium. In *Proceedings of the 12th international conference on Human computer interaction with mobile devices and services* (pp. 35-44). ACM.
- [68] Kafka, P. (2014, October 29). YouNow Is the Live Video Amateur Hour That Nearly Died. Now It's Booming. Here's How. *Recode*. Retrieved from <http://www.recode.net>
- [69] Khan, Z. C., Mashiane, T., & Shozi, N. A. (2015, February). Snapchat Media Retrieval for Novice Device Users. In *Iccws 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security* (p. 162). Academic Conferences Limited.
- [70] Kim, J., Klautke, H. A., & Serota, K. B. (2009). Effects of relational motivation and age on online self-disclosure: A content analysis of MySpace profile pages. Paper presented
- [71] Kongsved, S. M., Basnov, M., Holm-Christensen, K., & Hjollund, N. H. (2007). Response rate and completeness of questionnaires: a randomized study of Internet versus paper-and-pencil versions. *Journal of medical Internet research*, 9(3), e25.
- [72] Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing*, 13(6), 391-399.
- [73] Kujath, C. L. (2011). Facebook and MySpace: Complement or substitute for face-to-face interaction?. *Cyberpsychology, Behavior, and Social Networking*, 14(1-2), 75-78.
- [74] Kuss, D. J., & Griffiths, M. D. (2011). Online social networking and addiction—a review of the psychological literature. *International journal of environmental research and public health*, 8(9), 3528-3552.

- [75] Landgren, J., & Bergstrand, F. (2010). Mobile live video in emergency response: its use and consequences. *Bull. Am. Soc. Inf. Sci. Technol*, 36(5), 27-19.
- [76] LeSure, M. (2015). Adding Live Streaming Apps to Your E-Resource Arsenal. *Journal of Electronic Resources Librarianship*, 27(3), 199-201.
- [77] Li, K., Lin, Z., & Wang, X. (2015). An empirical analysis of users' privacy disclosure behaviors on social network sites. *Information & Management*, 52(7), 882-891.
- [78] Lillebo, O. K. (2011). Next generation privacy policy.
- [79] Lin, K. Y., & Lu, H. P. (2011). Why people use social networking sites: An empirical study integrating network externalities and motivation theory. *Computers in Human Behavior*, 27(3), 1152-1161.
- [80] Lockton, D., Harrison, D. & Stanton, N. (2010). *Design with Intent: 101 Patterns for Influencing Behavior Through Design*. Retrieved from [http://designwithintent.co.uk/docs/designwithintent\\_cards\\_1.0\\_draft\\_rev\\_sm.pdf](http://designwithintent.co.uk/docs/designwithintent_cards_1.0_draft_rev_sm.pdf)
- [81] Lockton, D., Harrison, D., & Stanton, N. A. (2010). The Design with Intent Method: A design tool for influencing user behaviour. *Applied ergonomics*, 41(3), 382-392.
- [82] Massimi, M., & Neustaedter, C. (2014, June). Moving from talking heads to newlyweds: exploring video chat use during major life events. In *Proceedings of the 2014 conference on Designing interactive systems* (pp. 43-52). ACM.
- [83] Mayer-Schönberger, V. (2011). *Delete: the virtue of forgetting in the digital age*. Princeton University Press.
- [84] Misoch, S. (2014). Card Stories on YouTube: A New Frame for Online Self-Disclosure. *Media and Communication*, 2(1), 2-12.
- [85] Misoch, S. (2015). Stranger on the internet: Online self-disclosure and the role of visual anonymity. *Computers in Human Behavior*, 48, 535-541.

- [86] Naghshineh, S., Ameri, G., & Zereshki, M. (2009). Human Motion Capture using Tri-Axial accelerometers.
- [87] Neustaedter, C., Greenberg, S., & Boyle, M. (2006). Blur filtration fails to preserve privacy for home-based video conferencing. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 13(1), 1-36.
- [88] Neustaedter, C., Pang, C., Forghani, A., Oduor, E., Hillman, S., Judge, T. K., Massimi, M. & Greenberg, S. (2015). Sharing domestic life through long-term video connections. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 22(1), 3.
- [89] Ngai, E. W., Tao, S. S., & Moon, K. K. (2015). Social media research: Theories, constructs, and conceptual frameworks. *International Journal of Information Management*, 35(1), 33-44.
- [90] Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when “privacy” matters. *Journal of Direct Marketing*, 9(3), 46-60.
- [91] Nowak, G. J., & Phelps, J. (1997). Direct marketing and the use of individual-level consumer information: Determining how and when “privacy” matters. *Journal of Interactive Marketing*, 11(4), 94-108.
- [92] O'Hara, K., Black, A., & Lipson, M. (2006, April). Everyday practices with mobile video telephony. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 871-880). ACM.
- [93] O'reilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & strategies*, (1), 17.
- [94] Oxford English Dictionary. (2007). *Privacy*. Retrived from <http://www.oed.com/viewdictionaryentry/Entry/151596?p=emailAYeCc.hcMKnYY&d=151596>
- [95] Padilla-López, J. R., Chaaoui, A. A., & Flórez-Revuelta, F. (2015). Visual privacy protection methods: A survey. *Expert Systems With Applications*, 42(9), 4177-4195.

- [96] Pearson, J. (2015, March 26). Periscope Could Have a Privacy Problem. Retrieved from <http://motherboard.vice.com/read/periscope-could-have-a-privacy-problem>
- [97] Periscope Help Centre. (2016). *How do I save my broadcast to my device?* Retrieved from <https://help.periscope.tv/customer/portal/articles/2017803-how-do-i-save-my-broadcast-to-my-device->
- [98] Petronio, S. (2012). *Boundaries of privacy: Dialectics of disclosure*. SUNY Press.
- [99] Pfeil, U., Arjan, R., & Zaphiris, P. (2009). Age differences in online social networking—A study of user profiles and the social capital divide among teenagers and older users in MySpace. *Computers in Human Behavior*, 25(3), 643-654.
- [100] Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, 19(1), 27-41.
- [101] Pierce, D. (2015, March 26). TWITTER'S PERISCOPE APP LETS YOU LIVESTREAM YOUR WORLD. *WIRED*. Retrieved from <http://www.wired.com>
- [102] Piwek, L., & Joinson, A. (2016). "What do they snapchat about?" Patterns of use in time-limited instant messaging service. *Computers in Human Behavior*, 54, 358-367.
- [103] Pötzsch, S. (2008, September). Privacy awareness: A means to solve the privacy paradox?. In *IFIP Summer School on the Future of Identity in the Information Society* (pp. 226-236). Springer Berlin Heidelberg.
- [104] Prabaker, M., Rao, J., Fette, I., Kelley, P., Cranor, L., Hong, J., & Sadeh, N. (2007, September). Understanding and capturing people's privacy policies in a people finder application. In *Proc. Workshop Ubicomp Privacy*.
- [105] Pullen, J. (2015, March 27). Periscope vs. Meerkat Which Is the Livestreaming App For You? *Time*. Retrieved from <http://time.com>
- [106] Raacke, J., & Bonds-Raacke, J. (2008). MySpace and Facebook: Applying the uses and gratifications theory to exploring friend-networking sites. *Cyberpsychology & behavior*, 11(2), 169-174.
- [107] Razali, N. M. & Wah, Y. B. (2011). Power comparisons of Shapiro-Wilk, Kolmogorov-Smirnov,



Lilliefors and Anderson-Darling tests. *Journal of Statistical Modeling and Analytics*, 2(1), 21-33.

- [108] Renaud, K., & Gálvez-Cruz, D. (2010, August). Privacy: aspects, definitions and a multi-faceted privacy preservation approach. In *Information Security for South Africa (ISSA), 2010* (pp. 1-8). IEEE.
- [109] Reponen, E. (2008, July). Live@ Dublin—Mobile Phone Live Video Group Communication Experiment. In *European Conference on Interactive Television* (pp. 133-142). Springer Berlin Heidelberg.
- [110] Roesner, F., Gill, B. T., & Kohno, T. (2014, March). Sex, lies, or kittens? Investigating the use of Snapchat's self-destructing messages. In *International Conference on Financial Cryptography and Data Security* (pp. 64-76). Springer Berlin Heidelberg.
- [111] Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., & Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in human behavior*, 25(2), 578-586.
- [112] Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., & Rao, J. (2009). Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing*, 13(6), 401-412.
- [113] Schaar, P. (2010). Privacy by design. *Identity in the Information Society*, 3(2), 267-274.
- [114] Segall, L. (2015, March 26). Meerkat who? Introducing Periscope. *CNN Money*. Retrieved from <http://money.cnn.com>
- [115] Shamma, D. A., Churchill, E. F., Bobb, N., & Fukuda, M. (2009, June). Spinning online: a case study of internet broadcasting by DJs. In *Proceedings of the fourth international conference on Communities and technologies* (pp. 175-184). ACM.
- [116] Sheehan, K. B. (2001). E-mail survey response rates: A review. *Journal of Computer-Mediated Communication*, 6(2), 0-0.
- [117] Shein, E. (2013). Ephemeral data. *Communications of the ACM*, 56(9), 20-22.

- [118] Shultz, K.S. & Whitney, D.J. (2005). *Measurement Theory in Action: Case Studies and Exercises*. Thousand Oaks, CA: Sage Publications Inc. ISBN: 0-7619-2730-1 -- particularly Module 5, or p. 69 - 73.
- [119] Shontell, A. (2015, March 26). What it's like to sell your startup for ~\$120 million before it's even launched: Meet Twitter's new prized possession, Periscope. *Business Insider*. Retrieved from <http://www.businessinsider.com>
- [120] SiteSell Blog. (2015, March 26). Everything You Need To Know About Twitter's Periscope. Retrieved from <http://www.sitesell.com/blog/2015/03/everything-you-need-to-know-about-twitlers-periscope.html>
- [121] Slonje, R., Smith, P. K., & Frisén, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, 29(1), 26-32.
- [122] Spiekermann, S., Grossklags, J., & Berendt, B. (2001, October). E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce* (pp. 38-47). ACM.
- [123] Stanley, B. (2015). *Uses and gratifications of temporary social media: A comparison of Snapchat and Facebook*. CALIFORNIA STATE UNIVERSITY, FULLERTON.
- [124] Stumpf, S., Rajaram, V., Li, L., Burnett, M., Dietterich, T., Sullivan, E., Drummond, R. & Herlocker, J. (2007, January). Toward harnessing user feedback for machine learning. In *Proceedings of the 12th international conference on Intelligent user interfaces* (pp. 82-91). ACM.
- [125] Stutzman, F., & Kramer-Duffield, J. (2010, April). Friends only: examining a privacy-enhancing behavior in facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1553-1562). ACM.
- [126] Subrahmanyam, K., Reich, S. M., Waechter, N., & Espinoza, G. (2008). Online and offline social networks: Use of social networking sites by emerging adults. *Journal of applied developmental psychology*, 29(6), 420-433.
- [127] Swerdlik, M.E. & Cohen, R.J. (1999) *Psychological Testing and Assessment: An Introduction to Tests and Measurement*. Mountain View, CA: Mayfield Publishing Co. -- particularly p. 150 - 151.

- [128] Thomas, L., Briggs, P., & Little, L. (2013, May). Location tracking via social networking sites. In *Proceedings of the 5th Annual ACM Web Science Conference* (pp. 405-412). ACM.
- [129] Trammell, K. D., Tarkowski, A., Hofmokl, J., & Sapp, A. M. (2006). Rzeczpospolita blogów [Republic of Blog]: Examining Polish bloggers through content analysis. *Journal of Computer-Mediated Communication*, 11(3), 702-722.
- [130] Tsai, J. Y., Kelley, P. G., Cranor, L. F., & Sadeh, N. (2010). Location-sharing technologies: Privacy risks and controls. *ISJLP*, 6, 119.
- [131] Tsai, J. Y., Kelley, P., Drielsma, P., Cranor, L. F., Hong, J., & Sadeh, N. (2009, April). Who's viewed you?: the impact of feedback in a mobile location-sharing application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2003-2012). ACM.
- [132] Usability Net. (n.d.). *Wizard of Oz*. Retrieved from <http://www.usabilitynet.org/tools/wizard.html>
- [133] Wang, J., Mughal, M. A., & Juhlin, O. (2015). Experiencing Liveness of a Cherished Place in the Home.
- [134] Wang, Q. E., Myers, M. D., & Sundaram, D. (2013). Digital natives and digital immigrants. *Business & Information Systems Engineering*, 5(6), 409-419.
- [135] Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011, July). I regretted the minute I pressed share: A qualitative study of regrets on Facebook. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (p. 10). ACM.
- [136] Weil, K. (2015, March 26). Introducing Periscope. Retrieved from <https://blog.twitter.com/2015/introducing-periscope>
- [137] Widjaja, N. D., Yeşil, S., Kaya, A., Ong, H. T., Ong, H. T., Rao, R. S., Murali Krishna, K., Ibrahim, L.M., Thanoon, K.H., Geumpana, T.A. & Koentjoro, J. (2012). Exploring user adoption of location-based social network in Indonesia. *International Journal of Information Technology and Business Management*, 6(1), 1-10.

- [138] Zhang, C., Rui, Y., & He, L. W. (2006, October). Light weight background blurring for video conferencing applications. In *2006 International Conference on Image Processing* (pp. 481-484). IEEE.
- [139] Zhou, H. (2015). Enhancing Mobile Content Privacy with Proxemics Aware Notifications and Protection.
- [140] Zywica, J., & Danowski, J. (2008). The faces of Facebookers: Investigating social enhancement and social compensation hypotheses; predicting Facebook™ and offline popularity from sociability and self-esteem, and mapping the meanings of popularity with semantic networks. *Journal of Computer-Mediated Communication*, *14*(1), 1-34.

## **Appendix A – Recruitment Notice**

### **Short text posted, for example, in a Twitter feed**

Researcher at Dalhousie U, Halifax, NS, Canada is looking for participants who are live video broadcasters.

([http:TBA](http://TBA))

### **Long text posted as the first page of Opinio**

We are researchers at Dalhousie University, Halifax, Nova Scotia, Canada conducting a study examining the usage of live streaming video apps (e.g., YouNow, Meerkat, Periscope). We are concerned about patterns of use and issues of privacy. We are looking for participants over the age of 18 and who broadcast using any live video broadcasting app. You will be asked to complete an on-line survey asking you about your usage and your perceptions of privacy and security. All of the collected data will be anonymous (and confidential), although we will collect a very limited amount of information about your background (e.g., age range, education). This survey will take 20-25 minutes to complete. There is no compensation for completing the study, but the collected data may lead to improvements in these apps.

If you are interested in participating, please continue for further information and to take part.

## **Appendix B – Consent Form**

### **Investigating the usage and privacy perception of temporal live video broadcasting apps**

**Principal Investigators:** Dhuha Alamiri, Faculty of Computer Science  
Dr. James Blustein, Faculty of Computer Science

**Contact Person:** Dhuha Alamiri, Faculty of Computer Science, dh481896@dal.ca

You are invited to take part in a research study being conducted by (Dhuha Alamiri, B.Sc.), a graduate student in the Department of Computer Science, as a part of my Master of Computer Science degree at Dalhousie University. The purpose of this research is to investigate the usage and privacy perception of live video broadcasting apps (e.g. YouNow, Meerkat, Periscope). We hope to learn how these apps are used, and what are the issues surrounding privacy. To be eligible to participate in the study, you must be at least 18 - years - old, and have used at least one of live video broadcasting apps at least once to broadcast a live streaming video (i.e., be a broadcaster).

As a participant in the research you will be asked to complete an on-line survey that is hosted on Dalhousie's Opinio software. You will be asked about your usage habits, reasons for use, and perceptions and preferences with respect to security and privacy features. This survey will take no more than 20-25 minutes. All responses will be saved on the secure Dalhousie's server and processed using statistical software.

Your participation in this research is entirely voluntary. Furthermore, if you choose to participate, you may end your participation at any time without penalty (by closing the browser). In addition, you may choose to not answer particular questions that you do not want to answer. At the end of the survey, there is a submit button. I will not include any surveys that are not explicitly submitted. However, if you do submit your survey and you change your mind later, it will not be possible to remove your data.

All the collected data is anonymous (and therefore confidential). The sum total of all the information that is collected will not be sufficient to identify you. You will not provide your

name, occupation, or financial information, or any exact details about your background (e.g., exact age, exact address, or exact education). The demographic data you provide is limited to age group, gender, education level, and approximate location (i.e., country and province). The data will be stored on a secure server and only the research team (i.e., myself and my supervisor) will have access to that data.

Results will be presented in “aggregate” form only (e.g., as averages or ranges). We will be examining the patterns of use, and the relationships between use, privacy/security, and demographics. The general findings will be presented in an academic conference or journal. I will destroy all information five years after completing the data analysis.

The risks associated with this study are no greater than those you encounter in your everyday life. The researcher is always available by e-mail to answer any questions you may have or address any problems that you may experience as you complete the survey.

There are no direct benefits for you from your participation in this research. You will not receive compensation. The research, however, might contribute to new knowledge on the use of such apps and on the privacy or security issues associated with such apps. This might lead to changes (i.e., improvements) in these apps or to the development of third-party apps that improve use of the apps.

You should discuss any questions you have about this study with Dhuha Alamiri. Feel free to ask as many questions as you like. My contact information is [dh481896@dal.ca](mailto:dh481896@dal.ca)

If you have any ethical concerns about your participation in this research, you may contact Research Ethics, Dalhousie University at (902) 494-1462, or email [ethics@dal.ca](mailto:ethics@dal.ca) (and reference REB file # 2015-3727).”

If you agree to complete the survey, read the following statement and check for “Agree”.

*“I have read the explanation about this study and have contacted the researchers for clarification if I had any questions and any questions have been answered to my satisfaction. I hereby consent to take part in the study and to have my anonymous responses quoted in reporting of the data. However, I understand that my participation is voluntary and that I am free to withdraw from the study at any time.”*

## Appendix C – Online Survey

### Demographic Questions

1. What is your age?

- a) 18-27 years old
- b) 28-37 years old
- c) 38-47 years old
- d) 48-57 years old
- e) 58-67 years old
- f) 68 years or older

2. What is your gender?

- a) Female
- b) Male
- c) Prefer not to answer
- d) Other

3. What is the highest degree or level of education you have completed?

- a) Less than high school
- b) High school graduate (includes equivalency)
- c) College or Trade School
- d) Undergraduate Degree
- e) Graduate Degree
- f) Professional Degree (e.g. medicine, law)
- g) Other (Please specify)

4. Where do you currently live? (Country and Province/State/ Region/District)?

5. What is your location of your childhood or family home? (Country and



Province/State/Region/District)?

6. How comfortable are you with technology:

1	2	3	4	5	6
Very comfortable	Somewhat comfortable	Comfortable	Somewhat Uncomfortable	Not comfortable	Very Uncomfortable
<i>I am the first to buy and others ask for help</i>	<i>I rarely need assistance</i>	<i>I use new technology, but may need help with set up and may need help with troubleshooting</i>	<i>I use it, but I do not like it</i>	<i>I need help often to use it</i>	<i>I avoid using technology</i>

7. How would you rate your knowledge of computer security?

- a) I have no knowledge at all.
- b) I have minimal knowledge.
- c) Good: I feel secure.
- d) Expert: I provide advice and assistance.

### Live Video Use

8. How often do you use the following live streaming apps for broadcasting live video?

	Periscope	YouNow	Meerkat	Other _____
Never				
Once a day				
Several times a day				
Once a week				
Several times a week				
Once a month				
Less than once a month				

*We asked this question to classify broadcasters based on the apps they use, so that only Periscope users can jump off to the third section later.*

9. Why did you start (or join) a live streaming video app? (Select all that apply)

- a) To maintain contact with friends I know online.
- b) To maintain contact with friends I know offline.
- c) To maintain contact with strangers online.
- d) To find new friends online.
- e) To find new followers/fans online.
- f) To advocate for change.
- g) To help people in need (e.g. who suffer from depression).
- h) To advice young people.
- i) To promote my professional profile.
- j) To promote my business or activities that I am involved in
- k) To promote my events or event that I am involved in.
- m) Other: \_\_\_\_\_

*This question was adopted from a survey conducted by Mosquera et al. (2012), who investigated the motivations of using social mobile applications to identify usage patterns of social app users. Answers (a), (b), (c), (d), and (e) derived from Courtois et al. (2013), who studied network public expectancies among YouTube video uploaders through an interview. We devoted answers (f), (g) and (h) for advocacy purposes based on observations of live video broadcasts where broadcasters present valuable content, providing suggestions or advice. We also created these options as a result of previous study (Misoch, 2014) who explored a phenomenon called card stories on YouTube through sampling of 25 YouTube videos (see section 2.3.2). Answer (i) was adopted and modified from Mosquera et al. (2012). Since creating a complete visible profile is not applicable in live video broadcasting apps, we modified it to be “to promote” to make it understandable to the participants (broadcasters). We derived the idea of Answer (j) from a study conducted an interview with YouTube uploaders (Courtois et al., 2013).. The idea of answer (k) was also taken from Courtois et al. (2013) and Mosquera et al. (2012) with the same purpose of using the word “to promote” as illustrated in the option (i).*

10. What types of content do you primarily broadcast, and to whom?

Content	Broadcast (Y/N)	Level of Visibility		
		Private (to one person)	Private (specific people)	Public (anyone on the Internet)
My formal presentations <i>e.g., my lectures or talks; my work or hobbies; my concerts or shows; my press conferences; interviews that I am involved in</i>				
My informal activities <i>e.g. me while clubbing, partying, drinking, dining, joking, entertaining; me while playing sports, music or talking; me while driving (dash-cam), etc.</i>				
The formal presentations of others (Semi-public) <i>e.g., their lectures or talks; their work or hobbies (e.g. sport); their concerts or shows; their press conferences; interviews that I am not involved in, etc.</i>				
The informal activities of others (Usually private) <i>e.g. others while clubbing, partying, drinking, dining, joking, entertaining; others while playing sports, music or talking; others while driving (dash-cam or regular); discussion of sexual activities of others, performance of sexual activities of others, etc.</i>				
Other <i>e.g., animals, nature, food, animation</i>				

*This question was constructed based on studies by Wang et al. (2011), who investigated type of*

posts that users regret on Facebook, Madejski et al. (2011), who categorized users intentions of showing or hiding information on Facebook profile page through a given table, and Rosener, Gill & Kohno (2014), who questioned about the type of sensitive content exchanged on Snapchat. The question was also based in part on Dextro, which is a computer vision company that dynamically scans and categorizes live video content of Periscope in order to make trending themes for brands, objects and scenes; lastly, it was also based on observations of live video broadcasts patterns during a period of one month. In order to explore users' self-disclosure behavior, we adopted the item "the level of visibility" from Mosquera et al. (2012). We modified it according to the level of visibility that exists in live video broadcasting apps (e.g., Periscope).

11. Are these broadcasts planned or spontaneous (unplanned)?

Content	Planned	Spontaneous
My formal presentations		
My informal activities		
The formal (planned) presentations of others		
The informal activities of others		
Other		

*The purpose of this question was to find out if the broadcast was planned, the broadcaster's level of self-awareness, and how likely the broadcaster is to engage in self-disclosure.*

12. Where are the majority of these broadcasts created?

Content	At Work	At Home	In Public Places	At Parties	Under influence of stimulants (e.g. alcohol)	While Driving
My formal presentations						
My informal activities						
The formal (planned) presentations of others						
The informal activities of others						
Other						

*The variable usage can be also described by the place or situation associated with that use (Boase & Ling, 2013). In addition, according to Misoch (2015), one of the factors that affects self-disclosure behavior is the situation in which the user is using computer-mediation communication.*

13. What are the emotions that accompany the majority of these broadcasts?

Content	Happy, excited	Sad	Angry, frustrated	Worried, anxious	Feel compelled to share	Not applicable required
My formal presentations						
My informal activities						
The formal (planned) presentations of others						
The informal activities of others						
Other						

14. How often do you broadcast when?

	Always	Often	Sometimes	Rarely	Never
Happy, excited					
Sad, depressed					
Angry, frustrated					
Worried, anxious					
Intoxicated (e.g. drunk)					
Feel compelled to share					
While driving					

15. Is your use of live video streaming apps restricted in any way? (Pick all that apply):

- a) No, because I use these apps as often as a need/want.
- b) No, because I have nothing more to share.
- c) Yes, because I do not have time to create more broadcasts.
- d) Yes, because I do not have any data plan or a small data plan for the Internet use.
- e) Yes, because I cannot afford the cost (e.g. bandwidth, proper equipment).
- f) Yes, because I am worried about security -- having my broadcasts "all over the Internet".
- g) Other \_\_\_\_\_

*The purpose of this question is to understand the reasons why some broadcasters use these apps less frequently than others*

16. Do you know that these apps do not enable the viewers to save the broadcasts?

- a) Yes.
- b) No.
- c) I know that Periscope allows one to save videos for up to 24hr (but the others do not).



17. Do you know that these apps do not enable the viewers to replay the broadcasts?

- a) Yes.
- b) No.
- c) I know that Periscope allows one to replay videos for up to 24hr (but the others do not).

*This question concerns the app chosen by the user. Since we are interested more in self-destructing or temporal live video broadcasting apps (e.g., Periscope), we added the third option because the third section of the survey is about Periscope.*

18. Using temporal live video streaming apps (e.g., Periscope, Meerkat), broadcasts are not permanently available on these apps for viewers. This is a positive feature because (choose all that apply):

	Yes
1. it keeps the contents of the broadcast secretive.	
2. it protects my privacy.	
3. it protects my intellectual property .	
4. it reduces the possibility that unwanted others will see my broadcast.	
5. it enables people forget facts about me.	
6. it helps to prevent strangers from making a profile about me.	
7. it minimizes how much data companies have about me.	
8. it protects the privacy of others.	
9. it minimize how much data companies have about others.	
of other positive reasons:	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

*Answers 1, 2, 4, 6 and 8 were derived from Shein (2013), who discussed the factors that make people use ephemeral messages -Self-destructing messages- as a communication tool with friends, and whether these data can be recorded somewhere.*

19. Using temporal live video streaming apps (e.g., Periscope, Meerkat), broadcasts are not permanently available on these apps for viewers. This is a negative feature because (choose all that apply):

	Yes, this matters
the content could be valuable.	
I cannot determine who watched my broadcast.	
it reduces the possibility that others will see my broadcast.	
I have to recreate my broadcast every time I need it.	
it causes (or enables) people to forget me.	
it limits the chance my broadcast to be popular.	
of other negative reasons:	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

20. In broadcasts, would you like to keep the following sensitive information private (choose all that apply)?

	Yes
My face	
My voice	
My exact location (e.g., GPS)	
My approximate location	
The visual of surroundings	
The people in my surroundings	
My inappropriate or atypical behavior	
The inappropriate or atypical behavior of others	
Other:	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

*This question is adopted and modified from Madejski et al. (2011), who surveyed the privacy attitudes of online social network users in order to develop recommendations for improving online social networks’ privacy settings.*

21. With respect to the ability to hide my face, I would like to conceal my face (choose all that apply-- you do not need to select any):

	Yes
1. because it could be used for identity theft. (e.g., SIN, Birthdate, address, and job).	
2. because it could help a predator or stalker find me.	
3. for professional reasons (e.g., employer would not appreciate my broadcasts, my broadcasts are incompatible with my type of employment or professional status).	
4. for social reasons (e.g., my broadcasts are incompatible with my social status).	
5. For personal reasons (e.g. I am not attractive enough).	
for other reasons: _____	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

*The question was adopted and modified from Madejski et al. (2011), who investigated the reasons behind hiding posted factual information (e.g., birthday, gender); we adopted options 1 and 2 from the question they asked and then created the rest of the options.*

22. With respect to the ability to distort my voice, I would like to conceal my voice (choose all that apply):

	Yes
1. because it could be used for identity theft.	
2. because it could help a predator or stalker find me.	
3. For professional reasons (e.g., employer would not appreciate my broadcasts, my broadcasts are incompatible with my type of employment or professional status).	
4. for social reasons (e.g., my broadcasts are incompatible with my social status).	
5. for personal reasons (e.g. I am not attractive enough).	
for other reasons: _____	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

23. With respect to the ability to hide my location, I would like to conceal my location (choose all that apply):

	Yes
1. because it could help a predator or stalker find me	
2. to avoid being found by people I do not want to see	
3. to prevent governments from tracking or monitoring me.	
4. for professional reasons (e.g., enabling my employer to track me)	
5. for social reasons (e.g., being judged on the locations I visit).	
6. for personal reasons (e.g. revealing activities that I am participating in).	
For other reasons: _____	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

*Options 2 - 6 are adopted from scenarios of risk-based sharing of location created by Tsai et.*

al (2010), who evaluated the user’s perceptions about benefits and risks of sharing-location technology, as well as the privacy controls associated with these technologies.

24. Please rate your level of concern for each of the following issues when you are broadcasting on the Internet:

	Very Concerned	Concerned	Not at all Concerned	Never though about it
1. Social reputation				
2. Physical harm <i>i.e., predators might learn of my location</i>				
3. Economic harm <i>e.g., identity theft</i>				
4. Others using or sharing my broadcasts without my consent (e.g., on Twitter or Facebook)				
5. Others taking a screenshot of my face or appearance				
6. Not knowing (or controlling) who views my broadcasts				
7. Not knowing (or controlling) who views my location				
8. Potential lawsuits from others in my broadcasts				
9. Potential employers can and will monitor my broadcasts.				

NOTE: The default option for this question will be “Not concerned at all”.

Issues 1, 2 and 3 of this question were adopted from Tsai et al. (2010), who addressed the most important reasons of online privacy. Issues 4 and 5 were adopted from Roesner et al. (2014),

who surveyed Snapchat privacy, while 6, 7, 8, and 9 came from Young and Quan-Haase (2009), who explored privacy concerns on social network sites.

25. With respect to feedback about viewers, I would like the app to (choose all that apply):

	Yes
notify me of who viewed my location (e.g., GPS coordinate).	
verify the identity of people who view my broadcast.	
verify the identity of people who follow me.	
provide an easy access to block a viewer who takes a screenshot of my broadcast or me.	
other options for privacy control: _____	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

## **Part II: Periscope Users**

*NOTE: This section will only be visible to those who have indicated that they have used the Periscope app.*

*Periscope is a live video broadcasting app, but has additional features that have do not exist yet in other similar apps. It saves the video on behalf of the broadcaster for viewers up to 24 hours. The video is deleted after that.. It also shows the precise location (e.g. GPS coordinate) of the broadcaster (if the broadcaster selects that option). Lastly, it is the only app that enables to broadcast privately to one or multiple users.*

26. How often do you broadcast privately to the following users?

	Always	Often	Sometimes	Rarely	Never
Family members					
Offline friends					
Acquaintances					
Online only friend (people I have never met physically)					
People I follow (am a fan of)					
People I work with					
Other:					

*The items of this question are adopted from Mosquera et al. (2012), who asked about the demographics of people's Facebook friends, in terms of how many are friends, family, etc.*



27. How often do you do the each of the following?

	Always	Often	Sometimes	Rarely	Never
Keep the broadcast available for 24 hrs					
Keep the broadcast available for less than 24 hrs					
Delete the broadcast immediately					
Other					

28. If you keep the broadcast available, why would you keep it available for replay?

	Yes
It can be useful.	
I like to review it.	
Viewers have requested it.	
I use it for view content (re-) evaluation.	
I use it for self-evaluation (e.g., quality of presentation).	
I want to know who the viewers are/were.	
I want to block viewers.	
I want to follow viewers.	
I want to obtain more feedback (e.g. comments or hearts) from viewers.	
Other: _____	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

29. If you delete the broadcast immediately, why would delete it immediately?

	Yes
Something embarrassing has been said about my physical appearance (i.e. face or body).	
There are inappropriately rude comments.	
There are inappropriate sexual comments.	
There are inappropriate comments or gossip.	
There are inappropriate or dangerous religious comments.	
There are inappropriate or dangerous political comments.	
I want to protect my privacy.	
I want to protect the privacy of others.	
I do not want it to fall into the wrong hands.	
Other: _____	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

30. With respect to the *show location* feature of Periscope:

	Yes	No
I know that Periscope shows my location (GPS) by default.		
I know that I can turn it on and off.		

31. How often do you reveal your location?

	Always	Often	Sometimes	Rarely	Never
While driving					
While creating other broadcasts					

*Questions 32 and 33 were adopted from risk and benefit scenarios related to sharing-location technology (Tsai et. al, 2010).*

32. What are the potential benefits of revealing your location while broadcasting (i.e., GPS)?

	Yes
Finding people in an emergency.	
Tracking people to ensure that they are ok.	
Parents can track their children.	
Providing directions to friends and family (facilitating a rendezvous).	
Tracking loved ones so to surprise them at a special event.	
The comfort of remote awareness of friends and relatives.	
So people can find me.	
Tracking my own activities.	
Others:	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

33. What are the potential risks of revealing your location while broadcasting (i.e., GPS)?

	Yes
Revealing the location of my home	
Being found by someone I do not want to see	
Being found when I want to be alone	
Revealing activities that I am participating in	
Being judged on the locations I visit	
Being stalked (e.g., sexual predators could use location information)	
Enabling the government to track or monitor me (e.g. texting while driving, speaking, etc)	
Enabling my employer to track me	
Others:	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

Thank you for your time: if you are willing to allow the use of your data, please hit SUBMIT. If not, you may simply close your browser.

If you have any questions about this survey, or if you would like a copy of the results when completed, then please make a note of the following contact information:

Contact Person: Dhuha Alamiri,  
 Faculty of Computer Science,  
 Dalhousie University, Halifax NS, Canada  
 Email: dh481896@dal.ca

## **Appendix D – Recruitment Notice**

We are conducting a study to evaluate our proposal designs of protecting the privacy of live video broadcasters. We seek members the Dalhousie University community (e.g., students, faculty, staff) who broadcast using any live video broadcasting software (e.g., Periscope) to help us evaluate our prototype designs. The study will be conducted in the Goldberg Faculty of Computer Science building (6050 University Ave).

You will be asked to provide consent, fill-in a short questionnaire about your background (e.g., education, experience with live broadcasting), and then interact with six prototype designs. Three of the prototypes that each tell you who is watching your location and where they are located. Each prototype will show the same information but each will show it differently. The second three prototypes will allow you different ways to set your privacy preferences in video broadcasting software.

The study will take about one hour to complete, and there is compensation of \$20 for participation.

If you are interested in participating, please contact

Dhuha Al-Amiri (Graduate Student, Dalhousie University)

dh481896@dal.ca

## **Appendix E – Consent Form**

### **Privacy Awareness and Design for Live Video Broadcasting Apps**

**Principal Investigators: Dhuha Al-Amiri and Dr. James Blustein, Faculty of Computer Science.**

**Contact Person: Dhuha Al-Amiri, Faculty of Computer Science, Dh481896@dal.ca**

We invite you to take part in a research study being conducted by Dhuha Al-Amiri at Dalhousie University. Your participation in this study is voluntary and you may withdraw from the study at any time. Your academic (or employment) performance evaluation will not be affected by whether or not you participate. The study is described below. This description tells you about the risks, inconvenience, or discomfort which you might experience. Participating in the study might not benefit you, but we might learn things that will benefit others. You should discuss any questions you have about this study with Dhuha Al-Amiri.

The purpose of the study is to help us learn effectiveness and usability of various privacy-aware interface designs for use while engaged in live-video broadcasting. You will be asked to participate in a 1 hour-long study where you will perform a set of tasks with 6 different prototype designs displayed on a cell phone and provide feedback regarding the usefulness of the design.

The first three prototypes deal with an interface designed to encourage individuals to think about privacy and security before broadcasting. The second three prototypes deal with providing the broadcaster (i.e., you) information about the locations of viewers.

Your participation is completely voluntary. You will be compensated \$20.00 for your time. This study will require about an hour to complete. You can withdraw from the study at any time without consequence. We believe that the risks associated with this study are minimal: no greater than those associated with everyday life. The researcher will be with you during the entire study should you have questions about the task. In addition, the researcher will be available while the study is active (e.g., several months around the time you participate) if you should have any additional questions.

At the beginning of the meeting, you will be asked to fill in a background questionnaire that provides general background information about age group, education group, gender, and experience with online live-broadcasting. Thereafter you will interact with three different prototypes. After interaction with each prototype, you will complete a questionnaire about your perceptions of understandability, likability, appropriateness, and effectiveness. After working with the three prototypes, you will rate the best. The process will then be repeated for the second three prototypes. (i.e., interact with each, rate each, rank all three).

All personal and identifying data will be kept confidential. Participant names and contact information will only be retained for the duration of the study. Thereafter, they will be deleted. The actual data will be stored anonymously (by participant ID number) in a secure location for 5 years post publication, or in accordance with journal requirements.

In the event that you have any difficulties with, or wish to voice concern about, any aspect of your participation in this study, you may contact Research Ethics, Dalhousie University at (902) 494-1462 or email: [ethics@dal.ca](mailto:ethics@dal.ca) (and reference REB file # 2016-3821)

- *I have read the explanation about this study. I have been given the opportunity to discuss it and my questions have been answered to my satisfaction. I hereby consent to take part in the study. However, I understand that my participation is voluntary and that I am free to withdraw from the study at any time.”*

### **Participant**

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

If you are interested in seeing the results of this study, please check below and provide your email address. We will contact you with publication details that describe the results.

*I would like to be notified by email when results are available for public viewing.*

[if this option is chosen, please include a contact email address: \_\_\_\_\_]

## Appendix F – Background Information

Participant ID: \_\_\_\_\_

1. What is your age?

- a) 19-23 years old
- b) 24-28 years old
- c) 29-33 years old
- d) 34-38 years old
- e) 39-43 years old
- f) 44 years or older

2. What is your gender?

- a) Female
- b) Male
- c) Prefer not to answer
- d) Other

3. What faculty you are involved in (if applicable)?

4. What is the highest degree of level of education you have completed?

- a) Did not complete high school
- b) High school graduate (includes equivalency)
- c) College or Trade School
- d) Undergraduate Degree
- e) Professional degree (e.g. Medicine, Law, Engineering, Architecture)
- f) Graduate Degree
- g) Post-graduate Degree (e.g. PhD, DLL)
- h) Other (Please specify)



5. How comfortable are you with technology:

- a) Very comfortable: I am the first to buy and others ask for help
- b) Comfortable: I use new technology, but may need help with set up and may need help with troubleshooting
- b) Somewhat comfortable: I rarely need assistance
- d) Somewhat Uncomfortable: I use it, but I do not like it
- e) Not comfortable: I need help often to use it
- f) Very Uncomfortable: I avoid using technology

6. How would you rate your knowledge of computer security?

- a) I have no knowledge at all
- b) I have minimal knowledge.
- c) Good: I feel secure
- d) Expert: I provide advice and assistance

7. How often do you use the following live streaming apps for broadcasting live video?

	Periscope	YouNow	Meerkat	Other _____
Never				
Once a day				
Several times a day				
Once a week				
Several times a week				
Once a month				
Several times a month				

8. Why did you start (or join) a live streaming video app? (Select all that apply)

- a) to maintain contact with friends I know online.
- b) to maintain contact with friends I know offline.
- c) to maintain contact with strangers online.
- d) to find new friends online.
- e) to find new followers/fans online.
- f) to advocate for change.
- g) to help people in need (e.g. who suffer from depression).
- h) to advice young people.
- i) to promote my professional profile.
- j) to promote my business or activities that I am involved in
- k) to promote my events or event that I am involved in.
- m) Other: \_\_\_\_\_

9. What types of content do you primarily broadcast, and to whom?

Content	Broadcast (Yes)	Level of Visibility		
		Private (to one person)	Private (to specific people)	Public (to anyone on the Internet)
My formal presentations <i>e.g., my lectures or talks; my work or hobbies; my concerts or shows; my press conferences; interviews that I am involved in</i>				
My informal activities <i>e.g. me while clubbing, partying, drinking, dining, joking, entertaining; me while playing sports, music or talking; me while driving (dash-cam), etc.</i>				
The formal presentations of others (Semi-public) <i>e.g., their lectures or talks; their work or hobbies (e.g. sport); their concerts or shows; their press conferences; interviews that I am not involved in, etc.</i>				
The informal activities of others (Usually private) <i>e.g. others while clubbing, partying, drinking, dining, joking, entertaining; others while playing sports, music or talking; others while driving (dash-cam or regular); discussion of sexual activities of others, performance of sexual activities of others, etc.</i>				
Other non-human activities, events, or scenes <i>e.g., animals, nature, food, animation</i>				
Other:				

10. Are these broadcasts planned or spontaneous (unplanned)? (Choose all that apply)

Content	Planned	Spontaneous
My formal presentations		
My informal activities		
The formal (planned) presentations of others		
The informal activities of others		
Other		

11. Where are the majority of these broadcasts created?

Content	At Work	At Home	In Public Places	At Parties	Under influence of stimulants (e.g. alcohol)	While Driving
My formal presentations						
My informal activities						
The formal (planned) presentations of others						
The informal activities of others						
Other						

12. In broadcasts, would you like to keep the following sensitive information private (choose all that apply)?

	Yes
My face	
My voice	
My exact location (e.g., GPS)	
My approximate location	
The visual of surroundings	
The people in my surroundings	
My inappropriate or atypical behavior	
The inappropriate or atypical behavior of others	
Other:	

*NOTE: The default option for this question will be “No”. Participants will only need to indicate which options are “yes”.*

13. People should be careful about their moods while broadcasting because (check all that apply)

- a) a person could make inappropriate comments while in negative moods.
- b) a person could engage in inappropriate or illegal actions while in negative moods.
- c) employers could be watching which could create a negative opinion of the broadcaster.
- d) strangers could be watching which could create a negative opinion of the broadcaster.
- e) friends could be watching which could create a negative opinion of the broadcaster.

## Appendix G – Questionnaire for Location Viewers Feedback Prototypes

### Asked While Viewing *Each* LOCATION VIEWERS FEEDBACK Prototype

Participant ID: \_\_\_\_\_



Start

1. In total, How many users are viewing your location? "If the app cannot do this, please skip"
2. Who viewed your location? "If the app cannot do this, please skip"
3. Which country/city they are belong to? "If the app cannot do this, please skip"
4. Where are the viewers of location located? "If the app cannot do this, please skip"
5. Who suddenly appeared on your list of viewers (started to view your location)? "If the app cannot do this, please skip"
6. Who suddenly disappeared from your list of viewers (stopped viewing your location)? "If the app cannot do this, please skip"
7. Who is the closest to your location? "If the app cannot do this, please skip"
8. Who is the furthest from your location? "If the app cannot do this, please skip"
9. Who is moving toward your location? "If the app cannot do this, please skip"
10. Who is moving away from your location? "If the app cannot do this, please skip"
11. Who moved towards and then away from your location? "If the app cannot do this, please skip"
12. How far is "Person X" from your location? [Note, person X is a variable.]
13. How far is "Person Y" from your location? [Note, person Y is a variable.]



End

**Asked After Viewing *Each* LOCATION VIEWERS FEEDBACK Prototype**

Participant ID: \_\_\_\_\_

14. Please rate your level of agreement with the following statements:

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
a) The purpose of the feature was clear.					
b) The announcement that viewers had examined “my” location was easy to obvious.					
c) It was easy to determine if viewers had examined “my” location.					
d) It was easy to find information about viewers.					
e) The information provided about viewers would be useful.					
f) The presentation of information about viewers was understandable at first glance (i.e., “intuitive”).					
g) It was easy to find the location of <i>specific viewers</i> .					
h) It was easy to find the identification of viewers at <i>specific locations (distances)</i> .					
i) It would be easy to continue broadcasting while checking viewer information.					



	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
j) Overall, the task was easy to perform.					
k) Overall, the task was understandable.					
l) Overall, the layout was nice.					
m) This feature would help me to feel more secure while broadcasting.					
n) This feature would remind me to reconsider my behavior about disclosing my location.					
o) This feature would add enjoyment to my broadcasts.					

Open-ended Questions:

15. What did you like about the task?
16. What do you dislike about the task?
17. Have you any general comments or suggested improvement about this task?

**Asked After viewing All LOCATION VIEWERS FEEDBACK Prototypes**

Participant ID: \_\_\_\_\_

18. Would you be likely to install an app that has this feature on your?

1. Yes
2. No
3. Maybe (please explain further)

Please feel free to record any additional comments here.

19. If an app like this was installed on your, would you use it?

1. Yes, regularly
2. No or very infrequently
3. Maybe / Not sure

Please feel free to record any additional comments here.

20. This type of app only provides information about people who *viewed your location*. Who would you want to know about?

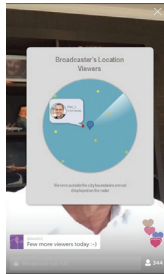
- A. Only those people who are in my city.
- B. Only viewers who are within a specific preset distance from my location.
- C. Any viewers from any location in the world.
- D. Other: \_\_\_\_\_

21. Presupposing you had to choose one, rank the three *location viewers* apps in terms of preference. You may rank them all the same.

Prototype 1: GeoLocate Prototype: Best -- Middle --- Worst.



Prototype 2: Radar plot: Best -- Middle --- Worst.



Prototype 3: GeoBar Graphical Prototype: Best -- Middle --- Worst..



22. Which features of a prototype are important? (You may choose more than one feature)
- a. the ability to monitor people who start to view your location
  - b. the ability to monitor people who stop viewing your location
  - c. the ability to see the closest person
  - d. the ability to see the furthest person
  - e. the ability to see the people moving toward your location
  - f. the ability to see the people moving away from your location

**The following questions are designed to allow you to provide additional information. You may write as much as you like. You may skip all of them if you like.**

23. Do you think the notification (if any) is useful? Why?
24. What do you like about prototype1?
25. What do you like about prototype2?
26. What do you like about prototype3?
27. What do you dislike about prototype1?
28. What do you dislike about prototype2?
29. What do you dislike about prototype3?
30. Do you have any general comments or suggested improvement?

## Appendix H – Questionnaire for Visual Privacy Awareness Prototypes

Asked After Viewing *Each* VISUAL PRIVACY AWARENESS Prototype

Participant ID: \_\_\_\_\_

1. Please rate your level of agreement with the following statement:

		Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
a) The task was easy to perform.						
b) The task was understandable.						
c) The overall layout was nice.						
<i>Imagine if you were to be in a good mood (e.g., happy, relaxed, calm):</i>	d) The task would be easy to perform.					
	e) The task would be understandable.					
<i>Imagine if you were to be in a bad mood (e.g., frustrated, angry, sad):</i>	f) The task would be easy to perform.					
	g) The task would be understandable.					
<i>Imagine if you were to be intoxicated (i.e., drunk, inebriated, using street drugs):</i>	h) The task would be easy to perform.					
	i) The task would be understandable.					

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
j) This feature would help me to feel more secure about my broadcasting.					
k) This feature would help me to be more aware of my behavior while broadcasting.					
l) This feature would help me to reconsider my behavior when broadcasting.					
m) This feature would add enjoyment to my broadcasting.					

Open-ended Questions:

2. What did you like about the task?
3. What do you dislike about the task?
4. Have you any general comments or suggested improvement about this task?

## Asked After Viewing All VISUAL PRIVACY AWARENESS Prototypes

Participant ID: \_\_\_\_\_

5. Would you be likely to install an app that has this feature on your phone?

1. Yes
2. No
3. Maybe

Please feel free to record any additional comments here.

6. If it was installed on your phone, would you be likely to use this feature?

1. Yes, regularly
2. No, or very infrequently
3. Maybe / Not sure

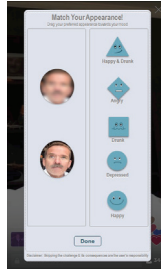
Please feel free to record any additional comments here.

7. Presupposing you had to choose one, rank the three *privacy protection* apps in terms of preference. You may rank them all the same.

A. Prototype 1: Matching mood-to-mood task Best -- Middle --- Worst.



B. Prototype 2: Matching your appearance-to-mood task: Best -- Middle --Worst.



C. Prototype 3: Choosing your appearance directly task:. Best -- Middle --Worst.

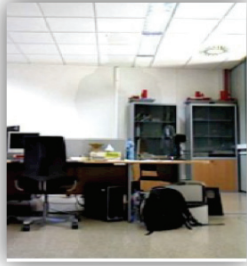


8. With respect to protecting your appearance, Which protection visual method do you prefer.



1. Blurring.





2. Hiding

Note that this could be an image of an empty room (as shown), or a landscape, or some other preset image.

3. No preference for blurring or hiding.

9. With respect to protecting the privacy of others while you are making self-broadcast, which protection method do you prefer?

1. Blurring

2. Hiding

3. No preference for blurring or hiding.

**The following questions are designed to allow you to provide additional information. You may write as much as you like. You may skip all of them if you like.**

10. Do you think the protection (if any) was useful? Why?

11. Do you have any general comments or suggested improvement?

## **Appendix I – Participant Payment Receipt**

### **Participant Payment Receipt**

My signature below confirms that I received a sum of \$20 (twenty Canadian dollars) cash from Dhuha Al-Amiri as an honorarium payment for participating in the “Privacy Awareness and Design for live video broadcasting apps” research project.

I understand this honorarium is taxable income and it is my responsibility to claim it on my income tax as Dalhousie University will not be issuing a T4A tax slip for this payment.

Name (please print): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_