2019

Individual Online Routines: External Guardianship, Personal Guardianship, and the Influence of Breaches

Ruby E. Booth

INDIVIDUAL ONLINE ROUTINES:

EXTERNAL GUARDIANSHIP, PERSONAL GUARDIANSHIP,

AND THE INFLUENCE OF BREACHES

by

Ruby E. Booth

A Dissertation

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

Major: Business Administration

The University of Memphis

August 2019

Dedication

For my father, I. Stanley Booth Sr., who loved me to the moon and back.

Acknowledgments

“We look…to the edges.” ~ Terry Pratchett

Behind every book is a story. In fact, behind every book is a whole passel of stories – one leading to another to another until the book becomes the one you have in your hand. An acknowledgements section can only tell a small fraction of those stories or else it becomes a book in itself. I’ll tell you parts of a few of the stories that went into this book, and then we’ll get on to the research.

In many ways, my story began long before I was born, when IBM sent a petite woman to repair a large machine at the Lincoln American Life Insurance headquarters in downtown Memphis, Tennessee. There, my daddy saw this small lady take out her tool kit and climb *into* the computer to fix it. He loved the incongruity of the image, and he told me the story many times. As I grew older, he encouraged me to find work I loved that I could make a living doing. Maybe climbing into computers would be it.

So, on a hot day in July of 2013, I found myself in the Fogelman Classroom Building at University of Memphis where I met a woman who would change my life forever. Judith Simon was then, and is now, petite and elegant with an easy laugh and a passion for security. I sat down in her classroom that first day not knowing if I belonged, not sure if returning to school, after a decade away, would be manageable for me. Luckily, Dr. Simon’s passion was contagious. By the end of that month, I had a whole new career trajectory and had somehow decided to spend my life learning scary new things.

I could also tell you a story about my partner, Mike Rowe, suggesting I get a hobby. A suggestion which led me to independent research and from there to the Ph.D. program. However, in deference to the rude absurdity of labeling five plus years of continuous grueling labor with a term reserved for frivolous relaxing, instead I will simply thank him for being the perfect partner for me. He supported this adventure, even though, having done it himself, he knew what it would cost us both in time, money, and sanity. He made many sacrifices, most invisible to me at the time, and continues to love and support me, even in our journey together to the other side of this huge country of ours. He is as much a hero, to me, as the characters in the comics he loves are to him. I love you, angel.

My advisor and committee chair, Sandi Richardson, has her owns stories. She kept me sane and on task through all the various permutations of my research process, more than once taking drafts of this work to meetings, doctors' appointments, and on one memorable occasion into her hospital bed. She also became my guide on matters of professional and sometimes personal ethics. She defended me from critics who told me I wasn't good enough for a doctorate—even when that critic was me. Without her patience and constancy, I would not have made it through. It is a debt I cannot pay; I can only attempt to do work worthy of her investment.

I am also indebted to Sandi for leading the best (and largest) damn dissertation committee the University of Memphis has ever seen. Dr. Brian Janz, Dr. Judith Simon, and Dr. Chen Zhang were our local members, providing support and signing the endless succession of documents necessary to get anything done. Dr. Stacy Petter and Dr. Michelle Carter guided me from afar. To sit on a doctoral committee from a distance is a particular challenge. At every conference we attended over the years, Sandi, Stacy, and Michelle carved out time to meet with me. Their comments, questions, and insight kept me from innumerable pitfalls. They challenged me to consider more deeply why this research was necessary, what it offered, and how best to perform it. My committee showed me that the smartest people you know and kindest people you know can be the same folks.

All through these years, my friends and family stood patiently beside me. Well, except for Joe Cotton, who stood by impatiently, asking, apparently daily, when I would be finished. Joe gave me two pieces of advice that allowed me to do this work. The second was: the time will pass anyway. The first was: bullshit! (His response to any suggestion that I wasn't smart enough for whatever obstacle stood in my way.) Martin Lambert offered a similar instruction, "I recommend arrogance," which I struggle to take every day. Benji Hughes simply provided the arrogance on my behalf, assuming I would be successful and would change the world for the better. A tall order I hope I can live up to. Nikka Valken has been beside me on all my life's travels, since I was 13 years old. Nikka is certain that I can do anything and has been since we first befriended alligators together all those years ago. I cannot imagine life without her in my corner.

I also couldn't have done any of this without my supers – three women who love and support me in all things –Amy Ellison, Christine Bertz, and Nikka Valken. They provide a cheering section, cave to hide in, and virtual home. They also remind me that, while we must sometimes visit Hell, we never build a summer home there. I must also thank the Cheese Fan club for eating cheese with me in good times and bad. They are Caroline Pate, Reagan Ryder, Kristi Swartz, Christine Bertz, Nikka Valken, and especially Christiana Leibovich whose reminders to keep writing combined with her confidence that I could do the thing, even if the thing was hard, helped me on many dark days.

Dr. Leanne Pate also helped on dark days, supported my struggles, and kept me rooted in the moment. I hope you are all lucky enough to find a therapist with her kindness and wisdom. I will miss her now that our time together is at an end.

Yo Clark kept body and mind together and functioning when I would have twisted myself into the most unproductive pretzels. I wish her full classes and a life free from suffering.

My fellow grad students made the way smooth where they could. Without Yao Shi, I would never have passed comps or the classes that let to them. Yao, Sungjin Yoo, and He Li got us all though seminars in which I would have exploded on my own. I will miss you, my sweet friends.

Finally, I am indebted, in innumerable ways, to my parents, of whom I am blessed to have many.

Gail and Dave are Mike's parents, but they have been rooting for me all the way as proud with me as if I was their own.

There for me since the beginning of all things, Michael Pittman has been there for all the updates, for long silences, for agony over drafts finished and unfinished, and finally for the glorious day I sent off the book itself. Whenever I had a moment of downtime, he was ready -- excited for all the "there I was" stories and sure to laughingly remind me, not to worry, that in a few hours or days I would have found a way to overfill my plate yet again. There is nothing on Earth like the pride I hear in his voice when he calls me: Dr. Honey. I am so lucky.

I thought I saw Bill Luton's biggest smile on the day I announced my intention to join the doctoral program. He toasted the ambitious plan with a huge grin. But I was wrong. The day I came in and announced, "I am now Dr. Booth." His face glowed.

My mother, Paula Townsend, has been with me for weeping and laughing. For emergency conference shopping and distracted lunches. For silences and rambling. She picks me first, when I need her, and it means the world. Mom, I couldn't have done it without you.

These are the people who make up my story. There are surely some I forgot, and others I could not fit without this becoming a book of its own. You all deserve more pages and more praise, but this will have to do. After all, we have research to discuss. I am so very grateful to you all.

With my deepest love,

Ruby E. Booth, Ph.D.

Abstract

Computer crime increases in frequency and cost each year. Of all computer crimes, data breaches are the costliest to organizations. In addition to the harm data breaches cause to organizations, these breaches often involve the exposure of individuals' personal data, placing the affected individuals at greater risk of computer crimes such as credit card fraud, tax fraud, and identity theft. Despite the breadth and severity of consequences for individuals, existing IS literature lacks coverage of how users respond to data breaches. Routine Activity Theory provides the study's theoretical frame. Routine Activity Theory states that crime occurs when the routine activities of a potential target place them in proximity to a motivated offender in the absence of a capable guardian. This work examines in detail the target-guardian dyad. Using semi-structured interviews, we inquire into potential antecedents to users' beliefs about external guardians, how users' beliefs about external guardians affect users' online routines, and how this process alters in the aftermath of a data breach.

This study employs a qualitative case study design to explore, at an individual level, the process by which users outside organizations determine their online routines, in light of their reliance for data protection on external guardians over which they have little to no control, and how the process is affected by awareness of a data breach. The cases selected are 1) the 2017 data breach at the consumer credit agency Equifax and 2) the Facebook Cambridge Analytica data compromise that became public in 2018.

Our findings show that users’ individual, situational, and data characteristics affect users' external guardianship beliefs and online routines. Additionally, under certain circumstances, users can fail to identify data guardians or develop adversarial feelings towards organizations that act as data guardians through control of user data. With some well-defined limitations, after data breaches users report changes in individual characteristics, perceptions of situational and data characteristics, and online routines. Based on these findings, we draw conclusions for future research and practice.

Table of Contents

List of Tables

Chapter One: Introduction

Research Problem

Computer crime, defined as illegal activity involving computers (Mumford 1998), increases in frequency and cost each year (Ponemon Institute 2017a). Of all computer crimes, data breaches, any “unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data” (Sen and Borle 2015, p. 315), are the costliest to organizations (Ponemon Institute 2017a). In addition to the harm they cause to organizations, when these breaches involve the exposure of the personal data of individuals, they place affected individuals at greater risk of computer crimes such as credit card fraud, tax fraud, and identity theft (Ponemon Institute 2017b).

In recent years, millions of Americans have had their data compromised when organizations in possession of their data failed to prevent illicit access to that data. A 2017 breach at the consumer credit agency Equifax saw 143 million consumer financial records stolen (Ponemon Institute 2017a), placing approximately half of the citizens of the United States at risk. Between 2014 and 2015, the data company Cambridge Analytica used Facebook to gain illicit access to personal data from 87 million people (Solon 2018). In this study, we examine the effect of organizational data breaches on individuals whose data was held by an organization and exposed during a data breach experienced by that organization.

Individuals affected by an organizational data breach may be consumers of an organization’s goods or services (as is the case with Facebook users), or they may be individuals about whom a company has gathered data as part of providing goods or services to third-parties (as is the case with Equifax users, whose individual data is part of Equifax's vast repository of consumer financial information). Regardless of the auspices under which an organization collects an individual user's data, these users face consequences from an organization's data breach. The consequences of a data breach to a user may include monetary losses, decreased value of the exposed personal data, increased probability of receiving spam, exposure of private information resulting in discrimination or social stigma, increased risk of fraud, increased risk of identity theft, and other psychological or intangible harms (Romanosky & Acquisti 2009, Baldwin et al. 2017, and Ponemon Institute 2017b).

Despite the breadth and severity of consequences for users, existing Information Systems (IS) literature lacks coverage of how users respond to data breaches. When faced with a wide range of possible negative consequences, we argue that users seek to reduce their likelihood of suffering such consequences in the future. The notification that their data has been compromised may trigger changes in user characteristics and perspectives that in turn affect their beliefs about external guardianship of their data, resulting in changes to their online routines. Users may change their online routines by altering their online activity; for example, choosing to abandon a social media platform. Users may change their routines by enacting personal guardianship behaviors, such as choosing more complex passwords. Note, we do not argue that such alterations in a user's online routine would necessarily achieve the goal of reducing their risk of being victim of a data breach. Rather, we assert that the process is itself of interest, whether effective or not, because it may change users' online behaviors.

Changes to user behaviors online have possible ramifications at many levels. Understanding how users adapt their behavior should enable scholars to better predict user choices in this period of frequent data breaches. Organizations could incorporate relevant findings into their marketing and service recovery strategies. Governments and security-oriented non-profits could use this information to develop relevant content for cybersecurity training materials. However, at present, IS security research has not captured the process by which users develop beliefs about external guardianship, how those beliefs affect their online routines, nor how breaches affect such beliefs.

This study examines, at an individual level, processes that lead to a user's online routines and changes that occur after a user becomes aware of a data breach. This topic offers value to the literature since the consequences of breaches on the beliefs, behaviors, and activities of affected users have received little attention, thus far, in IS research, but have applications for scholars, organizations, and governments (Bansal & Zahedi 2015).

Research Questions

Our research questions are:

1. How do individuals determine their personal online routines given that they are reliant for data protection on external guardians over whom they have little or no control?
2. How does awareness of a data breach impact this process?

Summary

This dissertation is laid out in six chapters. Chapter one introduced our problem space and our research questions. Chapter two will review the current state of IS security literature as it relates to our research; present Routine Activity Theory (RAT), which we use to frame our work, and describe the constructs we have chosen to employ in a tentative process model that we employed in our exploration of our research questions. Chapter three explains our choice of methodology, including case selection, sample recruitment, and our data collection processes. Chapter four covers our analysis of collected data with detailed descriptions of coding and categorization. Chapter five ties the results our data analysis to specific findings, answering our research questions and presenting propositions in the context of existing research. Lastly, chapter six offers our contributions to theory and practice, suggests possible future research, and describes the limitations of the study as executed.

Chapter Two: Literature Review and Theoretical Background

This chapter will cover IS research on security, the theoretical lens we will employ to frame our research, and our tentative process model combining the two. In the first section, we describe existing IS security research, providing an overview of the major research streams present at this time. In the second section, we introduce our theoretical lens, Routine Activity Theory, providing a detailed examination of its concepts and explaining their application to our research questions. Finally, in section three, we describe a model, derived from elements in IS security research and Routine Activity Theory, that we developed to assist in our exploration of our research questions.

IS Security Research

There exist three major, active streams of IS security research: 1) technological, 2) economic, and 3) socio-behavioral (Hua & Bapna 2013).

Technological

In IS security research, one of the major research streams, technological, formed when information security systems first appeared. Researchers began to develop technological solutions to guard against information security vulnerabilities. Using reference disciplines such as engineering and computer science, researchers in this stream created models of access control (Lockman and Minsky 1984), proposed algorithmic methods to improve the confidentiality of data in computer databases without compromising data integrity (Adam and Jones 1989), and identified key areas of computer-based vulnerability (Boockholdt 1989). Work on these technological solutions has continued to expand and evolve; this research is employed today by security professionals and used to create industry standards and federal regulations (Kwon & Johnson 2014). Unfortunately, no technological solution, no matter how well-designed, can provide perfect security for a system that contains human actors (Lee et al. 2016); humans inevitably introduce vulnerabilities. A technological stream of research is necessary, but researchers discovered that technology alone could not solve the problem of IS security. The efficacy of this research relied on the assumption that technology, once created, would be used by managers to prevent information security risks to organizations; this assumption turned out to be inaccurate (Marston et al. 1989). Managers often failed to implement these technological solutions either because they underestimated the necessity of these measures or lacked sufficient expertise in their use (Marston et al. 1989 and Straub & Nance 1990).

Economic

Another early stream of IS security research began with attempts to answer questions that would guide managers in their efforts to ensure computer-based information systems did not increase an organization's overall economic risks (Lockman and Minsky 1984). This stream was motivated by a desire to enable managers to rationally assess risks arising from organizations' increasing reliance on costly and sophisticated information systems (Rainer et al. 1991). Managers tended to underestimate the investment required to adequately secure their IS assets (Loch et al. 1992). Some IS security researchers argued that a firm's security investments should be selected based on economic risk modeling; these models combined qualitative and quantitative risk management methods previously used to assess other types of risk. (Rainer et al. 1991).

Unfortunately, at first, the efficacy of these risk management models was not empirically supported in an information security context (Baskerville 1991). Despite this lack of empirical validity, risk management models provided an important benefit: a lexicon.

In many organizations, management's adoption of sound information security policy was hampered by the lack of a common vocabulary between managers and security personnel. When describing information security, security personnel relied on highly technical terminology which managers rarely possessed the background to understand (Baskerville 1991). Risk management provided a shared language for discussions regarding the value of IS security investments, enabling technologically-skilled security staff members to convey the severity of risks and the benefits of investments to managers in a language that managers understood from their experience assessing other types of business risk. (Baskerville 1991). This demonstrated that a shared language regarding risks, costs, and efficacy can enable those without technical proficiency to make sound decisions about guardianship of their information systems.

Over time, the development and application of increasingly complex mathematic techniques overcame many obstacles to the predictive accuracy of risk management models in the information security context. Researchers extended and deepened existing models to allow the possibility of ambiguous outcomes characteristic of computer security (Sun et al. 2006). Improved simulations of attacker behavior were made possible through the use of game theory (Cavusoglu et al. 2008) and event studies (Png et al. 2008). Econometric modeling allowed researchers to assess the efficacy of different information security investments, including layered defenses (Cavusoglu et al. 2009), overt versus covert defensive postures (Cremonini & Nizovtsev 2009), and security outsourcing (Zhao et al. 2013). Despite this progress, the frequent introduction of unknown threats into the information security ecosystem limits the accuracy of economic models of information security risk (Straub & Welke 1998 and Dhillon & Torkzadeh 2006). Nevertheless, economic risk modeling informs managerial approaches to information security investment and has led to the creation of a host of options for organizations seeking to protect themselves from the financial risks of computer crime including cyber-insurance, third-party organizational security providers, and risk pooling (Zhao et al. 2013). While this stream of research has provided amply for organizations, the focus on firm-level dynamics has left the needs of private users largely unaddressed. Organizations have many options to offset information security risks, but users do not possess a corresponding toolset for the transfer, mitigation, or avoidance of information security risks.

Socio-behavioral

The final major stream of IS security research is socio-behavioral. Socio-behavioral IS researchers pull from the reference disciplines of psychology, sociology, and criminology. They examine IS security employing a schema in which organizations are viewed as a collection of responsible agents acting based on social norms and individual affordances (Backhouse & Dhillon 1996). This positions security within the realm of human decisions, thus allowing IS security research to encompass technical solutions, the efficacy of deterrents or preventative measures, and employee behaviors, all within the larger frame of choices made by individuals at work (Backhouse & Dhillon 1996, Phillips 1998, Straub & Welke 1998, and Willison & Backhouse 2006). This stream of research is of particular interest, in the context of our study, because it considers human decisions.

Socio-behavioral security research has shown that user's perceptions of security and interactions with security technology are affected by a variety of conscious and unconscious factors.

Conscious Factors

Conscious factors are those over which humans have active control. They encompass the choices we make day to day. While tied intimately with unconscious factors, conscious factors drive our behavior when we are attentively processing our environment (Kahneman, 2003). The conscious factors prior socio-behavioral research has identified as relevant to IS security are threat appraisal, fear, trust, and suspicion.

Threat Appraisal and Fear

IS security researchers have found that user's conscious decision-making when choosing whether to adopt protective technologies differs from the decision-making process individuals use for other technologies (Dinev et al. 2009). Evidence indicates that constructs found in the Technology Acceptance Model of "perceived usefulness" and "perceived ease of use," which generally influence adoption, are not significant in the context of IS security (Dinev et al. 2009). In the security context, individuals make an appraisal of threat based on their perceptions of their own susceptibility and the threat's severity (Liang & Xue 2009). Users do not adopt security tools if they underestimate their risks (Liang & Xue 2010) or overestimate the extent to which their self-efficacy in information security enables them to avoid harm without outside assistance (Herath et al. 2014).

Trust and Suspicion

Researchers have found that, when making decisions regarding online activity, users share information with sites they trust, and they are inclined to trust sites with visible security technology (Belanger et al. 2002). However, trust, when misplaced, can make users vulnerable (Algarni et al. 2017). Misplaced trust is a significant factor in phishing (Wright & Marett 2010 and Goel et al. 2017) and other types of social engineering (Algarni et al. 2017). The trust construct that has been empirically supported refers to situational trust between two parties, such as a customer and a firm, which is situated in a particular time and context, such as an online transaction to purchase goods.

In counterpoint to the trust, rather than referring to a specific decision, suspicion is understood as an ongoing assessment of others: a person with high suspicion does not anticipate beneficial conduct from others (Bobko et al. 2014). In their work, Wright and Marett employ dispositional factors of trust, perceived risk, and suspicion as relevant constructs affecting deception success in phishing attempts (2010). Individuals who have a high level of suspicion are less likely to fall for phishing attempts even when they trust the source of an email message (Wright & Marett 2010). Suspicion is distinct from both trust and distrust and is a process of three stages 1) uncertainty/ suspended judgement, 2) perception of malintent, and 3) cognitive activation (Bobko 2014). Evidence indicates that suspicion should be considered in addition to trust when modeling online behaviors, as it can be significant in situations for which trust is not significant (Wright & Marett 2010).

Unconscious factors

In addition to conscious factors, unconscious factors also affect users' perceptions of security and decisions about security behaviors. Unconscious factors are cognitive processes that we execute without any deliberate intention (Kahneman, 2003). Researchers have identified habituation and adherence to one's technological frame as unconscious factors that affect security behaviors (Anderson et al. 2016a, Anderson et al. 2016b, and Vuorinen & Tetri 2012).

Habituation

There are ways in which the brain works to undermine the user's ability to guard against harm. "Although users are frequently cited by security researchers as careless and inattentive [41], our results show that at least part of this behavior is obligatory and unconscious as a natural consequence of how the brain works." (Anderson et al. 2016b, P. 737). Faced with frequent warnings about possible threats, habituation inures users to the fear such messages are supposed to create; this particular cognitive process can be overcome with varying and increasingly garish messages, but it represents just one unconscious obstacle to sound security decision making (Anderson et al. 2016a and Anderson et al. 2016b). Similar to living next to train tracks, the consistent rumble of the engine and cars fades into the background with enough time. The same can be said for the appearance of warnings in the apparent absence of harm.

Technological Frame

Another unconscious factor that affects individual's interactions with security technology is the user's technological frame; a user's technological frame can be understood as the largely unconscious set of norms and ideas that develop around the use of an IT artifact

(Phillips 1998). The demands of guardianship can conflict with an individual's technological frame; for example, an individual whose technological frame includes an assumption of openness might expect to the access information within their organization freely– a behavior that would conflict with the implementation of sound IS security access controls (Smith et al. 2010). Individuals whose technological frame does not align with a particular security artifact may undermine or ignore that security artifact (Vuorinen & Tetri 2012).

In sum, the socio-behavioral stream of research demonstrates that users have conscious and unconscious individual characteristics (i.e., aspects of an individual's personality, character, or experience) that affect their security beliefs and behaviors. However, much of socio-behavioral IS security research focuses on specific aspects of a user's behavior: their adoption of technology, their decision to share information, their willingness to conform to security guidelines. Each piece described has value and provides insight, but none captures the entire process by which users determine their online routines.

Summary

Having reviewed the relevant aspects of technological, economic, and socio-behavioral IS security research, we find that existing IS security research offers wide-ranging findings on the use and adoption of security technologies, risk management techniques for managers in organizations, and evidence that user's perceptions of risk change their behaviors. However, it presently lacks coverage of the process by which users outside of organizations determine their online routines, and how the process is affected by a data breach.

Routine Activity Theory

IS security literature does not provide a solid theoretical foundation for understanding the processes by which users determine their online routines before and after learning of a data breach. However, data breaches are a form of crime, and a useful theory exists in the field of criminology. Routine Activity Theory (RAT) states that crime occurs when the routine activities of a potential target place them in proximity to a motivated offender in the absence of a capable guardian (Cohen and Felson 1979). These three actors form the ecosystems of crime; definitions of each can be found in Table 1.

Table 1: Routine Activity Theory	
Motivated Offender	A rational actor willing to commit a crime
Potential Target	A person, place, or object of value
Capable Guardian	A person or thing the presence of which deters an offender from committing a crime

Targets: a Caveat

The routine activities of targets place them in proximity to offenders increasing the likelihood that they will be victims of crime. In stating that a target’s choices place them in harm’s way, we do not place fault for the crime with the victim, nor intend to assert that there exists some perfect set of choices which would prevent a user from ever being victimized. In reality, much of a user’s data security is out of their hands. Once an organization possesses a user’s data, the user is affected by the choices about security made within that organization. Our research focuses on the Equifax and Facebook data breaches, both of which occurred in the United States where the current legal and technological climate allows organizations to collect information about individual users without their explicit consent (Hodges 2013). In such a climate, the user, no matter how skilled, must rely on organizations to guard them against data breaches. Such guardianship is external to the user and not susceptible to their personal control. Nevertheless, the users, as potential targets of crime, do possess some degree of autonomy and agency through their choice of online routine. Understanding how users determine their online routines, in light of their reliance on external guardians, could empower researchers, security application developers, and governments in any efforts they might undertake to support and facilitate users' personal guardianship behaviors and to reduce the risks to users that arise from their online activity.

Applicability to the IS Security Context

Prior IS security work demonstrates that RAT can be used within the IS field to understand aspects of computer crime (Willison & Backhouse 2006, Ransbotham & Mitra 2009, and Wang et al. 2015). For example, Willison and Backhouse found that local knowledge of an organization improves guardianship, because situational opportunities are important motivational factors for offenders who are inside an organization (2006). Wang et al. found a significant relationship between guardianship and targets and the likelihood of insider threats (2015). Ransbotham and Mitra identified two types of target selection which differ based on which target characteristics upon which the offender focuses (2009). This existing IS security research using RAT supports the use of the theory to answer questions relevant to our field but chiefly has been used to consider types of guardians, offender motivations, and characteristics that make targets attractive. By contrast, the perceptions, beliefs, and behaviors of targets (i.e., users) themselves have yet to be explored comprehensively and remain a fertile ground for research. In sum, there is a void in the IS security literature regarding users' perceptions, beliefs, and behaviors both pre- and post-breach. RAT can assist in our efforts to bridge this gap. We posit that RAT can apply to the context of user behavior online and how notification of data breaches affects this process. To our knowledge, this is first study to apply RAT to the process by which users outside organizations determine their online routines, in light of users' reliance on external guardians, and how the process is affected by awareness of a data breach.

The Target-guardian Dyad

In some ways, the relationship between an external guardian and potential target is paradoxical in the context of computer crime, since in this setting the user generally does not hire nor control their guardian. Users exist outside the organization. From their position outside, they are largely unable to affect organizational-level guardianship behaviors before or after data breaches. Indeed, since users may lack the ability to terminate the relationship with these guardians, as is the case with users and Equifax, one might assume external guardianship to be irrelevant to individuals' decision making. However, when studying the possible viability of a national identity ecosystem, IS researchers uncovered indications that individuals consider their beliefs about external guardianship when making decisions about their online routines (Crossler and Posey 2017). While users cannot control their data, they may make conscious decisions about their online routine based on their external guardianship beliefs.

In this study, we are concerned with the process by which users develop their online routines and how data breaches affect those routines; we seek to understand those routines in light of users' reliance on external guardians. Prior research indicates that users make decisions about their online routine based on their external guardianship beliefs (Crossler and Posey 2017). However, prior work has not addressed how those beliefs about external guardianship form. In this study, we examine in detail the target-guardian dyad; specifically, we explore specific individual characteristics that may be antecedents to users' beliefs about external guardians, how users' beliefs about external guardians affect users' online routines, and how this process alters in the aftermath of a data breach notification.

Relevant Antecedents to External Guardianship Beliefs

Existing research does not present a clear picture of how users develop external guardianship beliefs. In the absence of prior work on this specific relationship, we sought to determine possible antecedents to users' beliefs about external guardians. It was our hope to find constructs likely to apply, which we could use as a starting place when asking participants about their external guardianship beliefs. In an effort to identify these, we reviewed prior research in the security context to identify constructs previously shown to affect security beliefs and behaviors (Rountree & Land 1996, Rhee et al. 2009, Wright & Marett 2010, and Vance et al. 2014).

As part of our review of social-behavioral IS research earlier in this chapter, we discussed constructs that researchers have found to affect perceptions of or interactions with security. We discussed several constructs as part of that review: threat appraisal, fear, self-efficacy in information security, trust, suspicion, habituation to warnings, and technological frame. When we began to consider what the antecedents to external guardianship beliefs might be, these constructs were our initial candidates, because of their effect on security perceptions and behaviors found in other works. Reviewing these constructs for inclusion in our study, some constructs proved inappropriate to the research at hand, while others required restatement or refinement prior to data collection. In the following sections, we discuss all identified constructs in greater detail and explain our reasoning for their inclusion or exclusion.

Risk Perception

Introduced as a construct in Technology Threat Avoidance Theory, threat appraisal consists of two lower-order constructs: perceived susceptibility and perceived severity (Liang & Xue, 2009). Threat appraisal occurs when "users evaluate the potential negative consequences of being attacked by malicious IT" (Liang & Xue, 2009, p. 77). The threat appraisal construct is similar to an awareness construct introduced by Dinev and Hu: awareness of "potential threats and consequences of poor or no protection" (2007). Threat awareness has been shown to lead to fear (Dinev & Hu 2007). In the context of IS security, fear has been found to be more relevant than other constructs, such as perceived usefulness and perceived ease of use, which generally drive decision making with regards to technology (Dinev & Hu 2007). This finding is mirrored by fear appeals research using Protection Motivation Theory which considers fear to be a motivator of behavior (Boss et al. 2015). However, based on new findings from NeuroIS research that call into question whether the presence of fear can be accurately assessed by reflective measures and self-report, we are reluctant to employ either threat awareness or fear as standalone constructs (Warkentin et al. 2016). Thus, we have chosen to combine these associated concepts into a single construct of risk perception which should capture user awareness and appraisal of threat along with any emotional response thereto.

Self-efficacy in Information Security

Self-efficacy is a construct of long standing, arising originally from cognitive psychology (Bandura 1977). Self-efficacy is context specific, and the concept was adapted for the IS context in the form of computer self-efficacy, which refers to an individual's belief in their ability to perform computer-related tasks (Compeau & Higgins 1995). Self-efficacy in information security (SEIS) is a similar, but more recent, adaptation and is defined as "a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability" (Rhee et al. 2009, p 818). Researchers have found that SEIS significantly affects security perceptions (Wright & Marett 2010) and behaviors (Rhee et al. 2009). Individual's with higher SEIS perceive information security with inflated optimism; this optimism affects not only their self-assessment, but their assessments of others concerned with information security (Rhee at al. 2005). Based on the relationship between SEIS and individual's assessment of others, we have chosen to include this construct in our questions intended to identify antecedents to external guardianship beliefs.

Trust

Like self-efficacy, trust is a construct with a long history of use in IS research. The trust construct considers the relationship between two actors in which one actor believes that the other will act according to their expectations (Luhmann 1979). When adapted to the IS context, online trust was found to have important differences from offline trust. In specific, online trust involves both trust in the trustee (e.g., organization) and trust in the technology the trustee employs (e.g., their website) (Shankar et al. 2002). Through these two aspects, individuals assess whether the trustee is both willing and able to act as expected (McKnight & Chervany 2001a and McKnight & Chervany 2001b).

The IS security literature tends to look at trust mostly from the vantage of persuasion and deception (Wright & Marett 2010 and Wright et al. 2014). At times, in an IS security context, trust is presented as a single, unfaceted construct (Belanger 2002 and Wright & Marett 2010). This perspective informed our initial operationalization of trust in this work.

When conceptualized in this manner, trust had been found to have positive and negative effects on perception and behavior. Phishing messages are more successful at conversion when their recipient perceives the sender as trustworthy (Goel et al. 2017). Users who perceive a social media platform to be trustworthy are inclined to share more freely, which can have positive or negative implications (Tow et al. 2010). Trust also enables e-commerce (Belanger et al. 2002), improves organizational security compliance (Johnston et al. 2016), and decreases computer abuse (Lowry et al. 2015). Based on this evidence, at the outset of our research, we argued that a user’s inclination to trust is likely to affect their beliefs about external guardians and felt confident that trust could be examined as a single higher-order construct. We developed interview questions about relationships between trust as an antecedent to external guardianship beliefs based on this perspective. During data collection limitations to this approach became evident. We will discuss these issues in the upcoming subsection: Revisions during data analysis.

Suspicion

Suspicion as a construct originated in the field of communication with Interpersonal Deception Theory, which examines how individuals assess deception on a conscious or unconscious level (Burgoon et al. 1994). Variations of the suspicion construct have been employed in many fields. Across these fields, the construct tends to have three components: 1) suspended judgment, 2) concern about another entity's motives, and 3) cognitive activation (Bobko et al. 2014). Evidence indicates that suspicion should be considered separately from trust when modeling online behaviors (Wright & Marett 2010). When distinguishing between the two constructs, trust is characterized as a decision, while suspicion is an ongoing cognitive state (Bobko et al. 2014). It is possible for suspicion to be a significant construct even in cases where trust is not predictive (Wright & Marett 2010). A suspicious person does not anticipate beneficial conduct from others – a view we argue is likely to affect their perceptions of external guardians (Wright & Marett 2010). Therefore, we developed interview questions designed to reveal the relationship between suspicion and external guardianship beliefs. As with the trust construct, data collection revealed complexities around the construct of suspicion as described above. We will discuss these issues in detail in chapter four: Analysis.

Excluded Constructs

Habituation to Warnings

Habituation to warnings is another construct that appears in IS security research studying the user's perceptions of guardians (Zahedi et al. 2015, Anderson et al. 2016a, Anderson et al. 2016b, and Jenkins et al. 2016). However, habituation to warnings refers specifically to the narrow context in which protective software interrupts users with messages indicating possible security vulnerabilities; it does not refer to users' perceptions of external guardians in the sense of organizational guardians who possess user data. Thus, no questions intended to elicit user's habituation to warnings were developed for this study.

Technological Frame

The final construct covered in our review of potential antecedents based on prior research is the technological frame. This construct, which refers to the norms and ideas that form around an IT artifact, was introduced to explain the use of technology in organizations (Orlikowski and Gash 1994) and was applied promptly to an IS security context (Phillips 1998). However, there exist two obstacles to including this construct in our study 1) aspects of a technological frame are often unconscious or at least implicit and 2) a technological frame is a social rather than a purely individual phenomenon. (Orlikowski and Gash 1994). To include such a construct in our study would require an in-depth examination of user interactions in situ, which is outside the scope of this research. As such, no questions designed to isolate this construct were developed for our study.

Revisions during Data Analysis

During the process of data analysis, it became clear that two of our identified constructs, trust and suspicion, were inadequately distinct despite our initial attempts to choose stable and relevant constructs. Thus, it became necessary to broaden our literature review to include IS research on trust, distrust, and suspicion outside the IS security research context, in order to properly situate these constructs in their wide nomological network and resolve construct ambiguity.

During data analysis, we found that a higher order view of trust was insufficient to map our findings. Fortunately, there exists a rich stream of IS trust research outside of the IS security context. The work of McKnight and his collaborators was extremely helpful in clarifying our understanding of participant views on trust (McKnight and Chervany 2001b). Trust is presented as a multi-stage process (McKnight and Chervany 2001b). In order for trust to occur, users must also have the disposition to trust: a willingness to depend on others (McKnight and Chervany 2001b). They must have institution-based trust in the protective structures that exist within an environment (McKnight and Chervany 2001a). They must have trusting beliefs that the trustee is willing and able to act in their interests (McKnight and Chervany 2001a). These lead the trusting intentions and, ultimately, trusting actions.

Issues surrounding the trust and suspicion constructs are discussed more fully in our later analysis section, where they can be presented alongside the relevant data.

Summary

In closing, based on the arguments above, we identified four individual characteristics of users drawn from prior work likely to form antecedents to users' external guardianship beliefs. Specifically, we expected the individual characteristics of risk perception, trust, suspicion, and self-efficacy in information security to influence the development of users' beliefs about external guardianship. In the next section, we combine these constructs from prior IS security research with constructs in RAT to create a tentative model of the process by which users develop online routines in light of their reliance on external guardians and the effect of data breach on this process. We then used our model to develop an interview script designed to elicit the lived experience of users.

Model Description

To test our research questions, we define and contextualize our chosen constructs, describe the relationships between them, and depict those relationships in the form of a process model. The model can be found following our construct definitions in Figure 1. The constructs and relationships of this model provided a structure for the design of our interview script.

Constructs

Individual Characteristics

User's possess individual characteristics which we define as aspects of individual personality, aptitude, or experience. We have identified constructs that we argue comprise the individual characteristics affecting users' external guardianship beliefs. We define these constructs below.

- Risk perception is an individual's assessment of potential threats based on their online routine and any fear of computer crime victimization that they feel as a result of this assessment.
- Self-efficacy in information security (SEIS) is defined as "a belief in one's capability to protect information and information systems from unauthorized disclosure, modification, loss, destruction, and lack of availability" (Rhee et al. 2009, p 818).
- Trust is the user's expectation that an organization intends to provide guardianship and their expectation that the protective technologies that organization employs will be sufficient to execute that guardianship role.

- Suspicion is the perspective that others must be judged cautiously in an ongoing fashion because they are not intrinsically well-meaning. (Wright & Marett 2010 and Bobko et. al 2014).

External Guardianship Beliefs

In the preceding sub-section, we defined four individual characteristics from prior literature that we argue affect users' external guardianship beliefs. We will now define the construct of external guardianship beliefs.

Types of Guardianship

Computer crime researchers have subdivided guardianship into five levels, shown in Table 5: personal, physical, social, technological, and national (Yar 2005, Bossler & Holt 2009, Reyns et al. 2011 and Williams 2015). These divisions describe either the method of enacting guardianship, as is the case with physical or technological guardianship, or they describe the level of social order at which the guardianship is performed, as is the case with personal, social, and national guardianship.

Table 2: Types of Guardianship

Construct	Meaning	Operationalization	Works	Findings
Personal	A user’s ability to protect themselves from computer crime	Computer self-efficacy, willingness to share passwords, changing passwords, risk awareness	Bossler & Holt (2009)	Not Significant
			Williams (2015)	Significant only if country-level guardianship is excluded from model.
			Leukfeldt & Yar (2016)	Significant
Physical	The presence of target hardening measures	the presence of firewalls and security programs	Bossler & Holt (2009)	Not Significant
			Reyns, Henson, and Fisher (2011)	Significant
			Williams (2015)	Significant
Social	The presence of formal or informal online others who discourage criminal acts	On-site network admins, systems security staff, friends’ behavior, online peers, and industry self-regulation	Yar (2005)	Theoretically Supported
			Bossler & Holt (2009)	Significant
			Reyns, Henson, and Fisher (2011)	Significant
Technological	Any technology the presence of which discourages criminal acts	Antivirus software, firewalls, intrusion detection systems, profile tracking software	Yar (2005)	Theoretically Supported
			Reyns, Henson, and Fisher (2011)	Significant
			Leukfeldt, (2014)	Not Significant
			Leukfeldt & Yar (2016)	Not Significant
National	Mature national cyber-security strategies	Months since instantiation of national cybersecurity strategy, internet penetration	Williams (2015)	Significant

These divisions are well suited to the study of guardians; however, in research such as ours, which turns its attention to users, this level of granularity may not be appropriate. In the following section, we offer an alternate division of guardians that we believe is more appropriate to our research problem.

The argument for an External Guardianship construct

When a person makes a decision, they do not do so from an omniscient view of reality, but rather based on their understanding given incomplete information (Kahneman 2003). A person choosing what websites to visit or what information to share online will not always know which organizations hold their data or what forms of guardianship those organizations employ (Schneider 2009). While physical, social, technological, and national guardianship may affect the guardianship an organization provides, these forms of guardianship are not subject to separate assessment and alteration by users. Users are unlikely, for example, to know the extent to which an organization relies on social guardianship behaviors such as the presence of on-site network administrators. Nor are they likely to be aware which guardianship technologies an organization uses or how sturdy are the locks to the server rooms. In this way, all external guardianship, (i.e., any guardianship aside from a user's personal guardianship behaviors) forms a single, unknown whole. When undertaking this study, we anticipated that, in the absence of transparent and accurate knowledge, an individual's beliefs about external guardianship would be based on the user's individual characteristics.

User Online Routine

In the preceding sub-section, we presented a case for external guardianship beliefs. We argue that these external guardianship beliefs affect users' online routines. Now we will define the construct of users' online routine and the two lower order constructs of which it is composed.

Routine

RAT posits that we all have routines which place us in proximity to one another (Cohen and Felson 1979). These routines are composed of our day-to-day activities. The study of routines in relation to crime was brought into an online context by criminologists (Yar 2005). IS security researchers applied the construct to an organizational setting (Willison & Backhouse 2006).

Online Activity and Personal Guardianship Behaviors

Researchers using RAT have drawn a distinction between a routine online activity and an individual's personal guardianship behaviors; though both take place online, online activity and personal guardianship behaviors may change independently of one another (Leukfeldt and Yar 2016). Based on these findings, we have divided online routines into two lower-order constructs: online activity and personal guardianship behaviors.

- Online Activity refers to any actions an individual takes online that do not have a security motive; for example, the websites they visit, the content they post, games they play, etc. (Yar 2005).
- Personal Guardianship Behaviors consist of acts that an individual performs to keep themselves secure online, such as changing one's passwords regularly or studying common attack methods (Leukfeldt & Yar 2016).

Breach Announcement

A data breach is any "unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data" (Sen and Borle 2015, p. 315). In many countries, including the United States, laws and regulations dictate the circumstances under which an organization that experiences a breach must notify those whose data was affected (Hodges 2013). In addition, extensive media coverage of large breaches can also lead individuals to seek out information about a specific breach as well as whether their data was exposed in that breach.

Breach Notification

We consider a breach notification to have occurred when a user receives a notice from an organization through any media stating that their data has been affected by a security breach. We include both notices originating from the organization without user action and notices that are the result of an inquiry by the user. To illustrate, participants would be eligible for inclusion whether their notification occurred through an unprompted email from the breached organization or as a result of the user going to a website created by the breached organization to allow people to determine if their account was impacted. For the purposes of the Equifax case, we recruited participants who were notified of the data breach.

Breach Awareness

We consider breach awareness to have occurred when a user reports that they are aware of a specific data breach. This awareness can be the result of a breach notification, news coverage of a specific breach, television programs or podcasts discussing the breach, or any other means by which an individual gain knowledge that the breach has occurred. For the purposes of the Facebook case, we recruited participants who were either notified or aware of the data breach.

Effect on Users

We argue that breach awareness may affect users' perceptions, beliefs, and behaviors, resulting in changes to their online routines.

Research Model

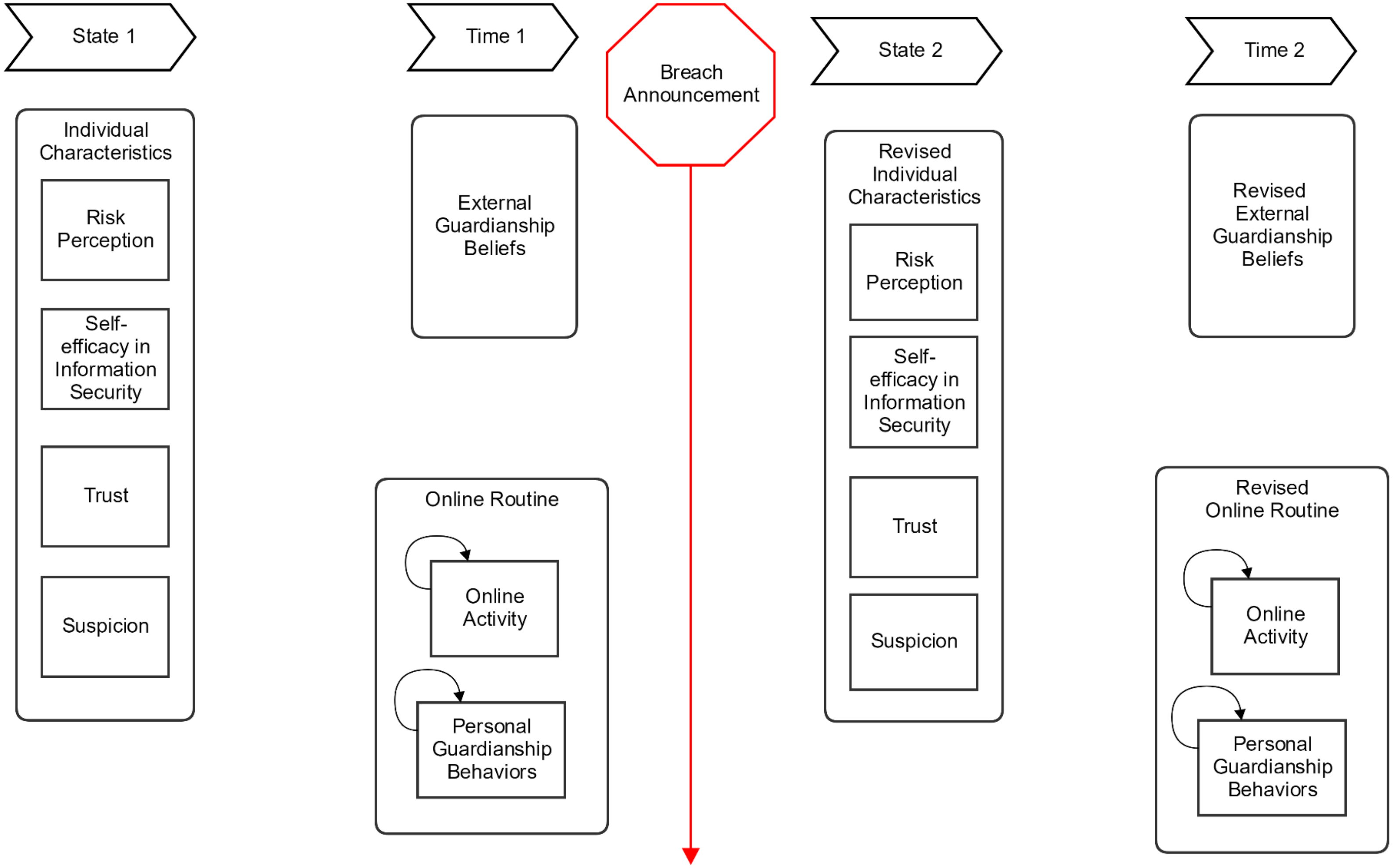

State 1
Individual Characteristics
Risk Perception
Self-efficacy in Information Security
Trust
Suspicion
Time 1
External Guardianship Beliefs
Online Routine
Online Activity
Personal Guardianship Behaviors
Breach Announcement
State 2
Revised Individual Characteristics
Risk Perception
Self-efficacy in Information Security
Trust
Suspicion
Time 2
Revised External Guardianship Beliefs
Revised Online Routine
Online Activity
Personal Guardianship Behaviors

Figure 1: Research Model

Summary

This chapter we have reviewed IS research on security, introduced the theoretical lens of Routine Activity Theory, and presented the constructs we determined likely to have relevance to our research questions. Finally, we provided a model, derived from elements in IS security research and Routine Activity Theory, that we developed to assist in our creation of an interview script to address our research questions. In the next chapter, we will give the scope of our research, discuss our chosen research method, and describe our sample selection process and our data collection methods.

Chapter Three: Methodology and Research Approach

Chapter Three will include a delineation of research scope, a discussion of the research method and its appropriateness to our research questions, a description of the research sample selection process and our data collection methods.

Research Scope

While Routine Activity Theory offers a foundation for a host of interesting research questions and future areas of research, the scope of this work is limited to RAT applied to the examination of antecedents to the beliefs of users about external guardianship, of how external guardianship beliefs determine users' online routines, and of how awareness of a data breach alters those processes for users who self-identified as affected by or aware of the Equifax or Facebook data breaches.

Methodology

The primary motivation for this study is the elaboration of Routine Activities Theory. RAT is not a new theory and has been applied to various contexts including those in IS security research (Willison & Backhouse 2006, Ransbotham & Mitra 2009, and Wang et al. 2015). Filling in gaps in existing theory (Pratt 2009); proposing relationships between existing theoretical constructs and new constructs (Edmondson & McManus 2007); and investigating new antecedents, moderators, or mediators to enhance the explanatory power of an existing theory (Ridder 2017) are all forms of theory elaboration, also called theory development (Pratt 2009 and Ridder 2017). Qualitative methods, in general, are appropriate for theory elaboration (Eisenhardt & Graebner 2007).

Qualitative methods are able to “offer insight into complex social processes that quantitative data cannot easily reveal” (Eisenhardt & Graebner 2007, p. 26). We chose to conduct a qualitative dual-case, interview-based research study to address our research questions. The qualitative case study, in specific, is a type of “empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident” (Yin 2003, p. 13). Case studies are suitable for research that seeks to answer “why” or “how” subjects respond to a given contemporary stimulus over which the researchers lack control (Yin 2018). Our research seeks to answer two “how” questions: “how do individuals determine their online routines given that they are reliant for data protection on external guardians over whom they have little or no control” and “how does awareness of a data breach impact this process.” Nor can we reasonably control the occurrence of a data breach without harm to our participants. Thus, our research meets the suitability criteria outlined by Yin (2018), and for these reasons, case study research is a fit for our study.

Case Selection

The selection of an appropriate case or cases is critical to the success of any qualitative case study research (Denzin & Lincoln 2011). As the focal point of a study, the case is a system bounded by time and activity (Creswell 2014). A case can be an individual, an entity, or an event (Yin 2018). Poetically stated, a case is a “quandary, that will invoke layers of understanding about the system” (VanWynsberghe & Khan 2007, p.81-82). More prosaically, a case is “a real world phenomenon with some concrete manifestation” (Yin 2018, p 77).

In our study, the cases selected are 1) the 2017 data breach at the consumer credit agency Equifax and 2) the Facebook Cambridge Analytica data compromise that became public in 2018. We have chosen two cases rather than one, because, while studies based on single cases offer value, multi-case studies allow deeper understanding of processes (Miles et al. 2014). Since our research questions seek to describe a process of user' determining online routines and any relationship between breach awareness and that process, a multi-case study seems appropriate.

We selected these instrumental cases, because they are typical of the population of data breaches in terms of types of data compromised; they also possess intrinsic significance due to the volume of affected users (Marshall & Rossman 2016). We have chosen two cases with broad similarities, but with some notable differences in their characteristics, in order to draw on another methodological strength of multi-case studies. Multi-case studies with differing, but similar, focal events allow for the emergence of common conclusions which provide evidence of generalizability (Yin 2018). Table 3 compares these two cases. In both cases, users experienced data breaches. However, the type of data compromised, the contrast in the voluntariness of user profile creation, and the manner in which the data compromise occurred represent differences. These differences hold the potential to reveal meaningful variations in perceptions, beliefs, and behaviors or, through the absence of such variation, provide initial evidence of model generalizability across breach types.

Table 3: Case Characteristics

Equifax	**Facebook**
Financial data affected	Personal and social data affected
143 million affected users	87 million affected users
Involuntary profile creation	Voluntarily profile creation
Data collected primarily via third parties	Data provided primarily by users and their social network
Data exfiltrated by hackers	Data sold to a third party, and then used in violation of the Terms of Service

Data Collection Method

Case studies can employ a variety of data collection techniques including interviews, participation in a relevant setting (e.g., spending time attending meetings at the focal organization), and analyzing secondary materials and artifacts (e.g., company memos or process documents) (Marshall & Rossman 2016). While some case studies rely on several types of data to triangulate findings, (Yin 2018), in-depth interviews alone are accepted as an efficient method of gathering rich, detailed data relevant to specific phenomenon (Eisenhardt & Graebner 2007). Interviews allow researchers to precisely delineate constructs and relationships (Eisenhardt & Graebner 2007). In-depth interviews offer the added benefit that follow-up questions and clarification of meaning can take place immediately during data collection (Marshall & Rossman 2016). Based on these merits, we selected in-depth, semi-structured interviews as our data collection method. Semi-structured interviews “allow the systematic and iterative gathering of data” (Eisenhardt & Graebner 2007, p150). The iterative aspect of this approach gives researchers an ability to adapt data collection as a study progresses and to combine inductive and deductive findings to create a more complete picture of existing dynamics within a problem space (Miles et al. 2014).

Sample

Our study examines the implications of two major recent security breaches: Equifax and Facebook. These cases represent the breach of two distinct types of data: 1) financial information and 2) personal and social information. The number of users who experienced these breaches were 143 million individuals and 87 million individuals, respectively (Ponemon Institute 2017a and Solon 2018). Based on recent findings regarding the optimal range of interviews in order to reach thematic stability, we recruited 12 users for each case (Marshall 2013).

Recruitment

To recruit participants, we employed a non-probabilistic approach combining participant self-selection with snowball sampling. This allowed us to capture the experiences of users affected by the phenomena of interest who were capable of providing descriptions of their experiences that were true to life (Miles et al. 2014).

Individuals were recruited via social media posts and emails to social and professional contacts. Internal Review Board (IRB) approved recruitment materials can be found in Appendix A. Digital recruitment messages included requests that recruitment messages be forwarded as widely as possible in an effort to minimize the incidence of ties between researchers and participants. Additionally, participants were asked to inquire amongst their social networks for possible eligible participants, as is typical in studies employing snowball sampling (Robinson 2014).

Inclusion Criteria

Our initial inclusion criteria were as follows: individuals must be 18 years of age older, residing in the US outside of incarceration, and report being notified of one or both data breach under study. Individuals who had worked for the organization experiencing the breach were excluded from selection. Inclusion criteria and demographic survey questions can be found in Appendix C.

After recruitment commenced, it became clear that the breach notification criterion posed a meaningful obstacle in the case of the Facebook breach. After reexamination of our research questions, we determined that expanding our inclusion criteria to permit individuals who were aware of the Facebook breach, but who were not notified of their own data being affected, would allow us to increase the pool of potential participants without sacrificing relevance. Subsequently participants were included who self-identified as “aware of” or “notified of” the Facebook breach.

Sample Demographics

In an effort to balance the need for sufficient data to achieve construct and model stability with need for parsimonious data collection in funded research, we recruited 12 users for each case (Marshall 2013). Some participants were eligible for inclusion in both cases. In these cases, participants were included only in the case for which they answered questions first. To protect participant confidentiality, each participant received an identifying code, which is used in research documents in lieu of names. Subsequent sections give demographic information by case.

Equifax Demographics

The sample gathered for the Equifax case included 12 participants: eight male users and four female users. Nine participants in the sample identified as White/Caucasian, one as Asian, one Black/African American, and one as Mixed Race. The majority of these participants were between 35 – 44 years of age and possessed a bachelor’s degree. Their median approximate annual household income was $100,000 - $149,999. Full details of participant demographics for the Equifax case are presented in Table 4.

Table 4: Equifax Participant Demographics

ID	Equifax	Gender	Ethnicity	Age	Education	Income
P001	Notified	Female	White	35 - 44	Bachelor's Degree	$35,000 - $49,999
P002	Notified	Male	White	35 - 44	Bachelor's Degree	$100,000 - 149,000
P004	Notified	Male	White	35 - 44	Bachelor's Degree	$200,000 or more
P005	Notified	Female	Asian	35 - 44	Graduate or Professional Degree	$150,000 - 199,999
P006	Notified	Male	White	35 - 44	Some college	$100,000 - $149,999
P007	Notified	Female	White	65 - 74	Bachelor's Degree	$200,000 or more
P008	Notified	Male	White	55 - 64	Bachelor's Degree	$75,000 - $99,999
P009	Notified	Male	White	55 - 64	Associate's Degree or Professional Certification	$200,000 or more
P010	Notified	Male	White	55 - 64	Bachelor's Degree	
P011	Notified	Male	Mixed Race	35 - 44	Some college	$50,000 - $74,999
P012	Notified	Male	White	35 - 44	Some Graduate School	$200,000 or more
P013	Notified	Female	Black or African American	45 - 54	Graduate or Professional Degree	$35,000 - $49,999

Facebook Demographics

The sample gathered for the Facebook case included 12 participants: six male users, five female users, and one non-binary user. Ten participants in the sample identified as White/Caucasian, two as Black/African American, and one White/Caucasian participant additionally identified as American Native or Alaskan Native. The majority of these participants were between 35 – 44 years of age. Participant education ranged from High School to Graduate or Professional Degree with the most common response being Graduate or Professional Degrees. The median approximate annual household income was $50,000 - $74,999. Full details of participant demographics for the Facebook case are presented in Table 5.

Table 5: Facebook Case Demographics

ID	Facebook	Gender	Ethnicity	Age	Education	Income
P003	Notified	Female	White	35 - 44	Graduate or Professional Degree	$150,000 - 199,999
P014	Aware	Female	White	35 - 44	Graduate or Professional Degree	$75,000 - $99,999
P015	Aware	Male	White	35 - 44	Bachelor's Degree	$35,000 - $49,999
P016	Aware	Female	White	35 - 44	Graduate or Professional Degree	$50,000 - $74,999
P017	Aware	Male	White	35 - 44	Graduate or Professional Degree	$35,000 - $49,999
P018	Aware	Female	White	65 - 74	High School	$100,000 - $149,999
P019	Aware	Non-binary	White and American Indian/ Alaskan Native	18 - 24	High School	Less than $25,000
P020	Aware	Female	White	35 - 44	Graduate or Professional Degree	$200,000 or more

Table 5: Facebook Case Demographics

ID	Facebook	Gender	Ethnicity	Age	Education	Income
P021	Aware	Male	White	35 - 44	Some college	$35,000 - $49,999
P022	Notified	Female	White	35 - 44	Some college	$100,000 - $149,999
P023	Notified	Male	Black or African American	25 - 34	Some college	$25,000 - $34,999
P024	Aware	Male	Black or African American	55 - 64	Bachelor's Degree	$50,000 - $74,999

Limitation of the Samples

We acknowledge that both self-selection and snowball sampling have known drawbacks. A limitation of these recruitment methods is that we are unable to report response rates to recruitment messages; since the number of individuals viewing the messages is unknown and outside of our control. Additionally, self-selection samples tend to bias towards candidates who are open, interested in the subject under examination, and female (Robinson 2014). Snowball sampling, which is dependent on social networks, can lead to the over-representation of socio-demographic sub-groups within the sample (Biernacki & Waldorf 1981).

We attempted to mitigate the potential biases of our sampling methods through purposive selection of those prospective participants who entered our selection process. However, our final samples for both cases illustrate the tendency of snowball samples to reflect the characteristics of those recruiting. This bias was particularly notable in terms of age and education. Across cases, 35-44 was most commonly reported age range, while, in the Facebook group, five participants reported holding a Graduate or Professional Degree. An oddity appeared in the Equifax sample. Though the median approximate annual household income was $100,000 - $149,999; the mode was $200,000 or more. This is not representative of national income demographics and may be an example of self-selection samples' bias toward individuals who are interested in the subject under examination. It may be that individuals with higher incomes are more concerned by and responsive to financial data breaches than individuals from other income ranges.

Instrumentation

When preparing for interviews, researchers must find a balance between unstructured, open-ended questioning and tightly structured questioning. The type of appropriate interview depends on the nature of the study. When a study examines a single case, is exploratory, and primarily inductive, open-ended questions work best (Miles at al. 2014). At contrast, in a study such as this one, which is driven by prior theory and involves multiple cases, a semi-structured question set focused on the constructs and relationships of interest decreases superfluous information collected and improves the efficiency and power of the analysis (Miles at al. 2014). Too much rigidity, however, is unwelcome and counterproductive. Semi-structured, rather than rigidly structured interview scripts are used, because they make it possible to delve into a participant's answers in order to identify underlying assumptions and to allow participants to explain ambiguous or unclear statements in their own words rather than relying on the researcher to assign meaning to their answers (Miles et al. 2014).

Our interview protocol went through several cycles of revision and review both by the research team and by the University of Memphis' Interval Review Board (IRB). This led to an interview protocol containing both questions highly specific to our model and questions intended to allow participants to provide information regarding their characteristics, perspectives, beliefs, behaviors, and experiences unanticipated by our theoretical foundation. Inclusion criteria and demographic survey questions can be found in Appendix C. Questions include demographic questions to address representativeness and qualification questions to ensure the appropriateness of the participant for inclusion as a study subject. The interview script itself can be found in Appendix D and takes the form of a semi-structured body of questions to test our chosen constructs and relationships. Appendix E illustrates just how the research questions map to the model.

Data Collection

Data collection took the form of semi-structured interviews with individuals notified of the Equifax breach or notified or aware of the Facebook breach. During these interviews, we employed an interview script (found in Appendix D) intended to elicit the user's individual characteristics, their beliefs about external guardianship, their online routines and the individual's reaction to the breach including any changes to their individual characteristics, beliefs about external guardianship, and their online routines made as a result.

Interviews took place at a suitable location or via phone, based on the participant's preference and practical considerations. Across the two cases, half of the interviews were conducted by phone and half face-to-face. In the Equifax case, seven interviews were face-to-face and five were online. In the Facebook case, five interviews were online and seven face-to-face. When conducting the interviews, questions were added or slightly rephrased to clarify participant responses and were omitted when the construct or relationship was fully addressed in response to a prior question. At the end of our script, we offered the users an opportunity to provide additional information on data breaches, breached organizations, or any other related insights.

All interviews were recorded and transcribed with the user's consent. Full consent document templates can be found in Appendix B. Once transcribed, interview participants were given an opportunity to review the transcripts of their interviews in order to confirm that the content reflects the words and intended meaning of the participants (DeMarrais 2004). Participant review of research material in this way is recommended to ensure data trustworthiness (Saldaña 2016). Additionally, participants were offered access to the final analysis, so that they may benefit from any findings that result from this inquiry, in alignment with contemporary perspectives on the ethical inclusion of participants in all phases of the research process, including its final benefits whenever possible (DeMarrais 2004). If ambiguity emerged in the process of data analysis, participants who consented to future communications could be contacted enabling them to provide clarification, if they desired.

Summary

In this chapter, we defined the scope of our research study as the elaboration of Routine Activity Theory through the examination of antecedents to the beliefs of users about external guardianship, of how external guardianship beliefs determine users' online routines, and how awareness of a data breach alters those processes for users who self-identified as affected by the Equifax or Facebook data breaches. The research method used in this study is a qualitative dual-case study using in-depth, semi-structured interviews, conducted either in person or over the phone, with users affected by one or both of two major recent security breaches: Equifax and Facebook. We recruited these participants using a non-probabilistic approach combining participant self-selection with snowball sampling. This gave us our data set of twenty-four user interviews. In Chapter Four, we will discuss data analysis for both cases as well as a cross-case analysis.

Chapter Four: Analysis

Introduction

The purpose of this study was to answer the research questions: 1) How do individuals determine their personal online routines given that they are reliant for data protection on external guardians over whom they have little or no control? and 2) How does awareness of a data breach impact this process? Our data analysis revealed six theoretical categories. Each of these play a role in the process by which users determine their online routines, in an environment where data breaches are common and users must rely on external guardians over which they have little or no control. This chapter will provide a thorough examination our data analysis process, the categories present in the Equifax case, how those categories differed or remained stable in the Facebook case, and a comparison of the cases.

Analysis

The data analysis methods employed in this study were derived from the best practices assembled by Miles, Huberman, and Saldaña (2014), whose guide to qualitative research has been widely adopted by researchers in the IS field and elsewhere. Our data analysis plan began with the creation of a code list deduced from our research model. These codes included all constructs and sub-constructs within the model:

- Individual Characteristics (IC)
    - Risk Perception (RP)
    - Self-Efficacy in Information Security (SEIS)
    - Trust

    - Suspicion
- External Guardianship Beliefs
- User Online Routine
    - Online Activity
    - Personal Guardianship Behaviors
- Breach Notification

In qualitative analysis, concepts often emerge from the interviews which do not fit the *a priori* constructs of one's chosen theory. Understanding this, we expected codes to emerge from inductive analysis of the interview data, in addition to our ten deductively derived codes. When unexpected concepts arose, we inductively coded the relevant data using *in vivo*, descriptive, or process coding as appropriate to the content, so that it could be included in second-stage categorical coding (Eisenhardt & Graebner 2007). These three code creation methods are defined as follows. *In vivo* coding uses the participants own words. It is useful in retaining the participant's voice and honoring their expression of lived experience (Miles et al. 2014). Examples of *in vivo* codes in our first round of coding included "trigger moment" and "I did not think about Equifax." Descriptive coding is another type of first-round coding we employed. To create descriptive codes, the researcher labels sections of text with words or phrases summarizing that content (Miles et al. 2014). Examples of descriptive codes in our first-round coding included "mandatoriness" and "data collection." Process coding was also used to show steps taken by users before and after data breaches. Process codes are gerunds (i.e., verbs functioning as nouns) used to show action within the data (Miles et al. 2014). Examples of first-round process codes include "tiering data." The process of coding each interview both inductively and deductively allows a thorough examination of relevant constructs and permits unanticipated constructs to emerge (Miles et al. 2014).

Addressing Data Quality

A Note about Solo Coding

While trustworthiness can be established in part through inter-rater reliability, team coding is not the only rigorous method of data analysis. Trustworthiness of a researcher's account can also be assessed by the steps a researcher takes when coding and analyzing. Multiple rounds of coding, pausing to write reflective memos, and confirming interpretations with participants are all methods of ensuring trustworthy findings (Saldaña 2016) By collecting data from a range of subjects, we hope to have captured some of the breadth of individual experience relating to the process of developing online routines and experiencing data breach through no fault of one's own. In the following passages, we describe the ways we have attempted to mitigate bias introduced through the use of a single data coder.

Credibility

Credibility refers to the accuracy with which researchers portray their participants (Bloomberg & Volpe 2019). We have endeavored to present the experience of our participants as accurately as possible. Participant interviews were recorded and then transcribed verbatim. After the interview, participants had the opportunity to check their transcripts for accuracy and to add more information if they desired. Through the data collection and analysis process, members of the research team met regularly to discuss study developments. Research memos created during the research process tracked emerging trends and difficulties in the data collection and analysis process. Participant summary memos were written using encoded initial transcripts. These memos have been included in Appendix G to allow additional depth in the reader's understanding of each participant. Finally, participants were given the option to receive the final research document; in this way, misinterpretations or misrepresentations can be corrected even after analysis.

Dependability

"Dependability refers to the stability and consistency of data over time" (Bloomberg & Volpe 2019, p 204). In this research, data was collected from February 22, 2019 to March 22, 2019. By keeping data collection in a fairly tight time frame, we avoid instability due to unexpected and impactful social, cultural, or political events. Data was coded iteratively in multiple rounds to reduce construct drift from the beginning of the coding process to the end.

Confirmability

Confirmability in qualitative research parallels objectivity in quantitative research (Bloomberg & Volpe 2019). We aspire to confirmability, not in the sense that we assert an unbiased and objective view of our research subject, but rather in the sense that our assertions should be clearly tied to and deeply grounded in data. We must acknowledge our biases and seek to faithfully present the methods, theories, and analysis that led us to our conclusions. It is our hope that we have accomplished this aim through the presentation of this research document.

Transferability

We designed this research project as dual case study with the intention of testing the ability to transfer the theoretical contributions from one case to the other. By examining two cases with similarities but notable differences, we could research common conclusions which demonstrate the ability to transfer our findings to new contexts (Yin 2018). To that end, we performed all analyses of the first case (Equifax) before analyzing the second case (Facebook). This process revealed areas of difference which may provide fertile ground for future research in the problem space.

Coding

The Equifax Case

Coding began by analyzing six of the twelve interviews in the Equifax case. Dividing the sample allowed us to test a variety of coding techniques to determine which best suited the data, research questions, and researcher ability. First all six transcripts were printed in hard copy and hand coded. The following represent a sample of insights that emerged in this first round of hand-coding. Some inductive codes appeared at once. Immediately the repetition of phrases such as “have to,” “make me,” and “no choice” indicated that mandatoriness was an issue of concern for users as they went about their online routine. Also featuring prominently were various forms of the phrase “no control.” This phrase described user control over data both as it went into the hands of Equifax from third-party sources and after data was in Equifax’s possession. Several users also perceived themselves as “the product” rather than “the customer” in their relationship with Equifax. Users expressed skepticism about any changes to Equifax’s security after the breach. They reported the view that Equifax would make “superficial changes,” due to fear of lawsuits and bad PR. These inductive codes occurred often enough that they held clear importance for the process under examination.

While inductive codes gained credibility through repetition, some pre-selected deductive codes appeared lacking. In initial coding, it became clear that “suspicion” could not be applied to both individuals and corporations as one construct. Participants consistently distinguished between their view of whether or not humans have other’s best interests at heart and their view of whether or not corporations have people’s best interests at heart. Participants varied in their suspicion of humans, while most felt that corporations always act in their own interests. Throughout the hand-coding processes, deductive codes were used where applicable, issues and difficulties with specific codes were written into memos, and new codes that emerged inductively during this process were added to a running code list.

Hand-coding proved useful but had its drawbacks. The sheer amount paperwork it generated could easily lead to concepts being overlooked. Paper-based analysis lacked an uncomplicated way to gather all similar codes together. Thus, the next round of coding used NVivo software.

Coding with NVivo

NVivo is a qualitative data analysis software package designed to enable researchers to store, organization, categorize, analyze, and visualize data in textual, audio, and video formats (QSR 2019). Transcripts of the first six Equifax interviews were imported into NVivo and coded using the code list deduced from our research model, as well as codes such as “no control,” “mandatoriness,” “the product,” “the customer” and “superficial changes” that arose inductively during hand coding. Analysis of each interview required new codes to capture relevant passages related to our research questions. These codes were expressed either *in vivo,* as direct quotations; as gerund-form process codes; or as descriptive phrases. Through coding participants P001 and P002, 50 codes appeared in the data, which added to the ten codes from the research model, gave us 60 codes. This is a normal part of open coding as many of these early codes collapse; though, some remain as new constructs to be included in the model (Saldaña 2016). Over time the number of new codes needed for each interview diminished. By the fourth interview there were 69 codes. By the fifth interview, there were 73 codes, with most new codes related to a decision to divide types of personal guardianship behaviors into subcategories such as passwords, limiting information given, and layered security. The sixth interview held steady at 73 codes. A full list of these first-round codes, along with their sub-codes, can be found in Appendix F.

Examining Codes

At this juncture, it seemed appropriate to examine the identified codes more closely. Qualitative analysis is an iterative process, as we have mentioned. One cycles from reading and coding data to examining codes and back again many times. However, at some point one's primary focus becomes, for a time, determining the meaning and value of the codes identified in the data as they stand in relation to the research questions proposed. "Just because something [in the data] is noticeable does not mean that it is meaningful or noteworthy in terms of [a] study's analysis" (Bloomberg & Volpe 2019). In order to determine which codes were relevant to the study at hand, we created a codebook following the design recommended in by Saldaña (2016). An example codebook entry can be found in Table 6.

Table 6: Codebook Example

Abbreviation	Work
Short Description	Work Background
Long Description	A participant’s current or past work environment or experience
Code Origin	Inductive
Revisions in code	No revisions
Inclusion criteria	Must be the participant’s work
Exclusion criteria	Second-hand assessment of fields
Typical Exemplars	e.g., “mostly, like, in the service industry, but based on my experience of working with people”
Atypical Exemplars	e.g., I think it is true of healthcare)
Close, but no	Not (e.g., My background is the humanities)

Researchers gave codes more concise phrasing, fully described codes, made explicit criteria for inclusion and exclusion in codes, resolved ambiguities between codes, and collapsed redundant codes. During this process, it became clear that some codes remained too large and amorphous to be useful, while other codes appeared sparsely and represented ideas or experiences not related to our study’s research questions. An example of the latter was “the dark web,” an *in vivo* code arising in a single interview. The phrase appeared at two points. One was a reference to a participant’s information “showing up on the dark web” and another was an explanation of why that occurred:

> “I probably think of the dark web more, because I occasionally get emails that I'm popping up on it. I mean, you know, a bunch of credit cards these days come with free monitoring. And so, you know, every once in a while, I'll get a pulse from, like, Capital one or Amex or whoever, just like you showed up on the dark web change everything.” (P006)

This material is relevant to our research questions only through the participant’s use of “free monitoring” and his reaction to the notices he receives (which is to do nothing different). Both of these are captured by other codes. Thus “the dark web” as a concept was not given an entry in the codebook, since it was deemed unlikely to arise as a meaningful theoretical component. Nevertheless, in a surfeit of caution, this encoding was retained in the dataset, since only half of the Equifax data and none of the Facebook data had been coded at that juncture. The code was left attached to the quoted phrases enabling researchers to include those early observations were "the dark web" to emerge as relevant later. Unfortunately, not all problems with these early codes were as easily resolved as "the dark web." Two constructs from our *a priori* model gave considerable difficulty.

Problematic Constructs

Trust and suspicion, two constructs from our initial model, proved problematic very early in the coding process. Overlap was common between the two constructs. Participants frequently used "suspicious" and "trust" without the clear discrimination between the concepts expected our review of prior research and indicated in our model. It was apparent that being "less trusting" of Equifax and being "suspicious" of Equifax were not distinct from one another as we expected from findings in prior work (i.e., Wright & Marett 2010).

Unexpected distinctions within the suspicion construct also arose. Our research question regarding suspicion asked individuals if they were "inclined to believe that people are generally out for their own best interests or that they generally have other's best interests at heart." People often had difficulty answering, because they did not see the two ends of that spectrum as mutually exclusive. One participant explained:

> "I think it's a combination of both, right? I mean, I think that's an interesting binary to put self-interest in, because I think that looking after the self-interest of one's self and looking after the self-interest of others is sort of in a lot of ways the

> same goal. Cause, like, looking out for your community, your community looks out for you.” (P001)

In addition, some participants emphatically clarified that, while they felt people had the best interests of others at heart, corporations absolutely did not:

> “I think somewhere between there. I mean, people I think are interested in other people’s well-being. Companies I think are very much— I'm very suspicious of companies in this definition of suspicion.” (P002)

Furthermore, a few participants distinguished between the behavior of individuals in groups versus individuals alone. One participant, P001, stated this clearly: “people, for the most part, are quite good, but once you get them in a group, they are terrifying.” Another, P002, expressed the belief that while a corporation would not care about his well-being, an individual within that company might be persuaded to care. “You know, if I talked to a person, they might be more interested in my wellbeing.” In short, suspicion lacked both convergent and discriminant validity at this point.

The trust construct, in itself, was also proving problematic. Not only did it easily overlap in participants’ minds with suspicion, but trust didn’t always align with the definition we assigned based on prior work in the IS security space (i.e., Shankar et al. 2002). As noted earlier in this work, we defined trust as “the user’s expectation that an organization intends to provide guardianship and their expectation that the protective technologies that organization employs will be sufficient to execute that guardianship role.” In our interview script this construct was measured primarily by the questions 1) “We trust companies to act in certain ways in certain situations. Prior to being notified about the breach, to what extent did you trust that [Equifax/Facebook] would be willing and able to protect your data?” and 2) “How did the notification affect your sense of trust that [Equifax/Facebook] would be willing and able to protect your data?”

Our expectation was that individuals would reply to our trust-related questions with conclusive responses, and we did receive some decisive answers. Trusting participants, like P005 discussing her view pre-breach, said, “I had a high level of trust simply because of their reputation.” Less trusting participants like P004 and P005 discussing their views post-breach said, “[the breach] definitely decreased my level of trust,” or “I have a lot less trust with [the] organization's ability to keep data safe.” There were some participants who felt trust or the lack of it very decidedly. However, alongside these clear-cut responses, we also heard more ambiguous answers: one participant, P002, said, “[the breach] did not affect my trust at all. I did not trust them to begin with. I had expectations and hopes, but I did not trust them.” Phrases like “I would hope,” “I hoped” or even “In the words of Fox Mulder, ‘I want to believe,’” from P005, arose repeatedly over the course of analysis. These phrases seemed to warrant further examination of the trust construct in this context.

Next, the second six Equifax interviews were coded to determine if the coding complexities arising from the first half of the data set were present in the second half. By and large, the data sets were similar. The overlap between suspicion and trust and the distinction between trust in people and trust in organizations were each present in the second six interviews. For example, when asked about their views post breach P009 said, “after it happened, of course, I was more suspicious of [Equifax], and would be less trusting of them.” The distinction between companies and humans were present in phrases such as “individuals are gonna have a lot more motive for protecting your things than a company would," from P008. Given the persistence of these issues, it was clear that revision and restatement would be necessary to clarify our codes.

Reexamining Trust and Suspicion in IS Literature

At the suggestion of a member of our research team, we made a closer review of IS literature on trust and distrust outside the IS security space. As mentioned in chapter two, the work of McKnight and his collaborators quickly revealed a more nuanced view of trust, the process of trust development, and associated sub-constructs. McKnight shows trusting behaviors as having antecedent beliefs. The trust model has been elaborated on and expanded over time, but a simple, early version is shown in Figure 2.

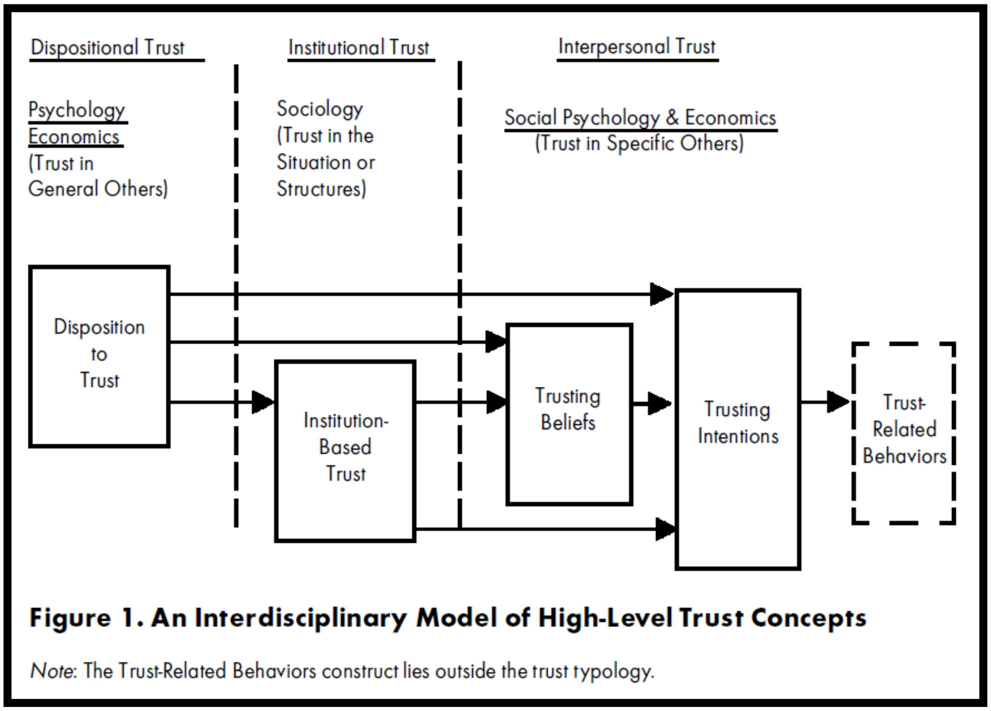


Figure 1. An Interdisciplinary Model of High-Level Trust Concepts

Note: The Trust-Related Behaviors construct lies outside the trust typology.

Figure 2: Trust Model from McKnight, D. H., and Chervany, N. L. (2001b). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. International journal of electronic commerce, 6(2), 35-59.

The high-level trust model separates trust into stages. Disposition to trust is the “extent to which a person displays a tendency to be willing to depend on others across a broad spectrum of situations and persons” (McKnight et al. 2002, p. 339). This construct can be further decomposed into “faith in humanity” and “trusting stance.” Faith in humanity is when “one assumes others are usually upright, well meaning, and dependable” (McKnight et al. 2002, p. 339-340). Trusting stance describes the perspective that “regardless of what one believes about peoples’ attributes, one assumes better outcomes result from dealing with people as though they are well meaning and reliable” (McKnight et al. 2002, p. 340). Institution-based trust deals not with trust between people, but with trust in a situation. For example, institution-based trust would be present when an individual feels confident that laws and regulations are in place to protect them from harm within a given context (McKnight et al. 2002). It also decomposes into two sub-constructs “structural assurance” and “situational normality.” Structural assurance is the belief that “protective structures – guarantees, contracts, regulations, promises, legal recourse, processes, or procedures – are in place” (McKnight and Chervany 2001a, p. 37). Situational normality is the belief that a “risky venture is normal or favorable or conducive to situation success” (McKnight and Chervany 2001a, p. 38). In combination, these antecedents lead to trust in specific others. In context of our study, for example, someone might tend to believe the best in people and to rely on them (high disposition to trust). They may also believe that there are laws and regulations in place that protect them when sharing data with financial companies online (institution-based trust). These together may lead them to feel confident in trusting a specific company such as Equifax. Armed with these additional constructs, we returned to the Equifax case data.

Participant Summary Memos

Coding data, by its nature, fragments participant's narratives (Bernard et al. 2016). When coding, a researcher focuses on small meaningful slivers of a participant's responses. When this work is done well, these slivers, combined with other slivers, begin to form patterns that illustrate the lived reality of participants in a research context. However, it can be easy in the coding stage to lose sight of the overall narratives from which these data points are drawn. In an attempt to stay grounded within the users' real experiences, at this point, participant summary memos were created for all twelve of the Equifax participants. These memos included a brief demographic description of the participant and a condensed participant narrative written using a combination of quotations from interview transcripts and the researcher's own descriptions. The memos can be found in full in Appendix G. The writing of these documents served to re-anchor the analysis in the real-world experiences of users from which the data arose.

The Facebook Case

In the Facebook case, coding took place in NVivo. The initial codes were drawn from the code list of the Equifax case. As before, six of the twelve interviews were coded, then the codes were assessed to determine what refinement they needed.

Examining Codes

Eight new codes arose from the first six Facebook interviews. Of these seven were related to user online routines: automaticity of Facebook use, decreased use, not linking or unlinking accounts, leaving the mobile app, leaving Facebook, leaving other social media, and restricting third party apps. The remaining code created was “distrust of information,” a code that refers to users greeting information online with distrust due to the prevalence of fraudulent or ill-intentioned accounts and sources. All of these codes seemed relevant, concise, and within scope for our research questions. Thus, no substantial revisions were deemed necessary. The stability of the coding structure gave us confidence that this code list was appropriate to the data (Rubin & Rubin 2011). As a result, the remaining six interviews were coded without returning to the literature for clarification.

New Inductive Codes

When coding the final six Facebook interviews, five new codes emerged. Two of the new codes were simply types of personal guardianship behaviors. “Incognito browsing” refers to a browser feature that suspends browser tracking of one’s activity. “Limiting interaction” refers to choosing not to have conversations online; P019 explained their use of this behavior as “I don't really interact because I don't want people seeing me.” Another code that emerged was an individual characteristics sub-code “prior experience of online harassment.” This code mirrors the code “prior experience of fraud” found in the Experian case; data breaches on social media can lead to harassment or stalking in an analogous manner to a financial breach leading to experiences of fraud. The final code that emerged was a sub-code of situational characteristics: “no competition.” This code refers to the lack of substitutes for firms like Facebook as well as the firm’s immense size and market dominance.

Participant Summary Memos

As with the Equifax case, upon completing first-round coding, we returned to the users' full interview transcripts. After reading and listening to these, participant summary memos were created for all twelve of Facebook participants. These memos included a brief demographic description of the participant and a condensed participant narrative. Several participants expressed strong emotions regarding the Facebook breach, its effect on their lives, and its implication for the world. Even more than the Equifax summaries, writing these memos proved important in re-grounding the research in real-world lived experiences of users that these interviews and codes represent. The memos can be found in full in Appendix G.

Categories

The process of initial coding and then category refinement is central to sense-making in qualitative research (Miles et al. 2014). After coding, we grouped our existing codes into categories, beginning with the Equifax case. These categories consist of constructs from routine activities that arose in the data as well as themes/constructs that emerged from inductive coding. This ability to combine inductive and deductive findings to create a more complete picture of existing dynamics within a problem space represents one of the great strengths of qualitative methods (Miles et al. 2014).

The six categories that emerged were: Individual Characteristics, Situational Characteristics, Data Characteristics, Breach, External Guardianship Beliefs, and User Online Routine. In following sections, we provide definitions of and support for these categories.

Individual Characteristics

Based on prior research in the security context, we expected that individual characteristics of users would affect users' external guardianship beliefs and online routines. Our analysis supported two constructs from prior research as relevant: risk perception and self-efficacy in information security. However, as noted earlier in this work, trust and suspicion proved insufficiently precise to serve. Instead, a new construct was employed: beliefs about human nature. This construct manifested with two sub-constructs "faith in humanity" and "suspicion of humanity." Another construct emerged as relevant to users' security beliefs and behaviors: work background.

Risk Perception

All participants discussed their view of risk, and participant risk perspectives covered a wide range. Some participants felt fairly secure about giving their data to companies operating online, such as P008 who said, "I didn't see it as that risky for the most part" and P007 who said, "I didn't think there was a risk." Some participants felt the risk was more moderate, such as P012 who stated, "on a scale of one to ten with ten being the most risky, I would say probably a six." On the other extreme there were participants such as P006 who described the risk of giving away data as: "Nightmarishly awful in all cases."

Self-efficacy in Information Security (SEIS)

All participants discussed their view of SEIS, and these assessments included statements such as P004 saying, "I don't know if I ever had necessarily a great amount of faith in my ability to predict my data online." In contrast with P012, who said "I would say more than average in competence…. I felt like because I could assess the risk, I could make the right choice."

Beliefs about Human Nature

Subject beliefs about human nature as expressed could be described by two sub-constructs: "faith in humanity" and "suspicion of humanity." The majority of participants described themselves as more suspicious of humanity, with statements including P010's "Everyone's a potential danger" and P012's "I would say that I'm probably more suspicious. Altruism is not an innate thing." Three participants described themselves as having faith in humanity. Examples of this include P001 saying "And I just kind of trust the people who are good at that to do their best," and P002 saying "I mean, I think people in general are good. I'm not too suspicious of them."

Work Background

The final individual characteristic that recurred in the data was participant work background. Half of the Equifax participants used their experiences at work as a comparative benchmark when assessing Equifax and its security practices. P007 provides an example: "I thought that most companies were as secure as the company I work for and because we take security so important." P010 expressed a similar sentiment: "I mean, I've done a lot of work in the medical profession. My last job was at Baptist, and it's like data is sacred."

Situational Characteristics

Another category that emerged during analysis was one which we have chosen to call "situational characteristics." Based on participant interviews, factors related to the context (i.e., situation) of creating online routines affected users' security decision-making. McKnight's institution-based trust construct seemed, at first, to describe these participants' views. Institution-based trust is, in essence, trust in the structures and conditions that enable success in a particular situation (McKnight and Chervany 2000). We wondered, though, whether institution-based trust had relevance in the case of Equifax given the fact that users could not chose to exclude their data from Equifax's guardianship. "Freedom to act is assumed in trust relations," (McKnight and Chervany 2001a); yet, in data collection, participants used phrases expressing their sense of powerlessness, such as "no control", "had to", and "made me". Half of participants used language reflecting a sense that they felt Equifax was a mandatory part of their experience. For example, P004 said, "they're sort of the evil, you know, you can't do without." Another participant stated:

> The one that I know I've been hit was Equifax, which is incredibly frustrating, because that's not a voluntary service. You know, I've never given [them] my information. That's one that they are given by others for me having the privilege to take part in economy. (P006)

Furthermore, two-thirds of participants reported feeling no control over Equifax and its data collection. Users expressed a lack of control over their data once Equifax was in possession of it. Even when they felt as though Equifax might protect their data, they still expressed frustration at the lack of agency over their own information. P001 described it as, "I think there's sort of a definition of protection. Like, they weren't asking us what we wanted them to do with it." Another participant expressed a variation on this sentiment:

> I can only control what I have access to, right? So, saving my information into a website, that is my choice. That is something that I could control. I don't know

> that I've ever seen where a bank says you can opt out of having your information online. So, there's no opt out there. (P005)

Trust assumes freedom to vary one’s actions (McKnight and Chervany 2001). Thus, the overall institution-based trust construct, which requires freedom to act and implicitly freedom to refrain from acting, was not a good fit to our data. On the other hand, most participants did express some trust in what McKnight and others have called structural assurance, a sub-construct of institution-based trust. Structural assurance refers specifically to a belief in the protective structures present in a situation that contribute to good outcomes (McKnight and Chervany 2001).

Many participants expressed a belief that fear of negative consequences such as lawsuits encouraged companies to keep data safe. P005 said, “I assumed that they can sue. So, most organizations want to avoid lawsuits. So that keeps them on the straight and narrow.” P013 agreed with this: “So wherever the legalities of how they get to sued fall into place, they will rub up against those. Regardless of whether it's ethical or not.”

Some participants argued for regulatory intervention to improve security in the future.

> I'm not a fan of big government, but obviously some things do have to be regulated. I would say that that's the case where regulation could be good is if a company ... It costs them dollars to obviously protect that data, and maybe they were trying to not spend those dollars. Therefore, maybe if they'd been a little more protective, and we'd had some regulations in place, then they would have had to spend those dollars. (P009)

Overall, participants expressed the belief that adverse consequences for failure to protect user data would result in improved guardianship of user data over time.

In sum, the category of situational characteristics is a part of the process we seek to understand. Within this category, participants reported that their perceptions of mandatoriness, lack of control, and structural assurance affect their beliefs and behaviors.

Data Characteristics

Another inductively derived category that appeared was data characteristics. Target value is a construct present in much of Routine Activity Theory research (Cavusoglu et al. 2008 and Png & Wang 2009). Researchers have found that directed attacks are motivated by diverse types of value including tangible value, iconic value, or reprisal value. (Ransbotham & Mitra 2009). We did not expect a value construct to arise in our research, because in prior works target value has usually assessed by the offender (Cavusoglu et al. 2008, Png & Wang 2009, and Ransbotham & Mitra 2009) or the guardian (Wang et al. 2015), rather than the target. Nevertheless, such a construct did appear, as users assess their data's value to themselves, to offenders, and to guardian organizations.

Examples of participants views include P009's discussion of the amount of data Equifax held, "I would of thought they would have been one of the most trustworthy agencies because they have so many people's data." P007 argued that data sensitivity demanded specific protective actions: "They have so much sensitive data that they should have had secured servers." P002 compares the likelihood of someone targeting Equifax's store of data versus his own: "Obviously, since they have so much financial and sensitive data, they're going to be targeted more than, for example, me."

Some users reported assessing the value of their data. Some users also placed value on the mass of data held by organizations. While only half the Equifax participants discussed data characteristics, all who did argued that data characteristics were important to the calculus of security. These assessments of data affect users' perceptions of risk, their beliefs about what constitutes appropriate action on the part of external guardians, and their willingness as users to commit to personal guardianship behaviors.

Breach

This construct was present in our original research design as "breach notification." It was modified to include "breach awareness" in order to overcome obstacles to participant recruitment. Our Equifax participants all received notice from Equifax through some media stating that their data has been affected by a security breach. Facebook participants included users who self-identified as either "aware of" or "notified of" the Facebook breach

During data collection a few interesting facets to the breach construct emerged. Learning of a breach was explained as an inciting incident, or "trigger moment."

> I mean, I changed my passwords that one time. It was sort of like a trigger moment where I, you know, what? I should probably do that. And since then it's been consistent. So, I really, I haven't in my mind chalked it up to Equifax. (P002)

Further, the number of breaches that a user had observed in a certain time prior to the breach under examination could result in action when one breach would not.

> You know, based on prevalence of the hacks in last two years, maybe not this one specifically. I have changed the way I do passwords. I've started using grammatically correct sentences. (P006)

Finally, users attended to the delay between when a firm became aware of a breach and when that firm notified users. When users deemed the delay between discovery and announcement lengthy, users felt less favorably about the firm.

> I was really glad [Equifax] notified me. I can't remember the timing on when they sent the notification versus when the hack happened. I seem to recall, there might have been a delay. I may be thinking of a different one, but I thought there was a slight delay. In when they notified versus... I understand they want to get all the information together to really understand what exactly happened and how many accounts were affected. Um, but I always feel like there's a responsibility to notify people as soon as possible. (P005)

> [Equifax] didn't immediately notify people. They found out they'd been breached, they sat on it, they tried to fix it, they tried to sweep it under the rug, instead of just owning it, which I don't think a company today would do that. Because there have been enough breaches now that you're not going to find a company that's going to feel the need to sweep it under the rug. (P012)

Not only does awareness of a breach trigger changes to a user’s perspectives and behaviors, but participants report that the manner in which a breach is announced and the prevalence of other breaches in the same time period also influences their experience.

External Guardianship Beliefs

Initially, we defined external guardianship beliefs as a user’s beliefs regarding any guardianship aside from that user’s personal guardianship behaviors. We further argued that these external guardianship beliefs would reflect a view of external guardians as a single unknown whole. The guardian-target dyad is central to our research questions. Individuals rely on these guardians but have little to no control over them. Nor do users have visibility into any guardianship behaviors other than their own. We began this research deeply curious as to what would emerge related to this dynamic.

According to the data, prior to the breach, the majority of participants did not have external guardianship beliefs about Equifax. Three-quarters of participants either were not aware or did not think about Equifax having a role in protecting their data. Of those who did consider Equifax as a data guardian, only one, P012, reported a change in their view of Equifax as a result of the breach. However, P012 had prior work experience related to Equifax, which affected his initial view of the firm’s guardianship. After the breach, users rapidly developed views of Equifax as inadequate.

Participant P004 expressed the consensus view well:

> I don't know, like, I don't think I ever really thought about it. I knew they had an enormous amount of data. I knew that getting a hold of what was in my credit report and confirming that it was accurate was an unfortunate consequence of them having a lot of data and having sort of that role in our society.… But yeah, I don't think I spent any time thinking about, like, what kind of security they might have in place. Or even thinking about the fact that they would be a relatively detrimental target if someone did target them…. But again, like it was never as a company I interact with directly. I didn't have firsthand knowledge of what their security practices were…. I guess they went from not having a perception necessarily to having a perception that they suck (P004),

In sum, the majority of participants in the Equifax case did not have external guardianship beliefs about Equifax, but after the breach, users developed largely negative views of Equifax as a data guardian

User Online Routine

Drawing on Routine Activity Theory, we included in our interview script questions about the construct “user online routine” as composed of two sub-constructs: “online activity” and “personal guardianship behaviors.” Based on prior literature, we defined online activity as actions a user takes online without a security motive (Yar 2005). Also based on prior literature, we defined personal guardianship behaviors as acts an individual performs to keep themselves secure online (Leukfeldt & Yar 2016). Both sub-constructs of user online routine appeared in our data.

Online Activity

Online activity presented exactly as expected, with users’ readily describing their daily, weekly, monthly, and even yearly routines online. All participants willingly disclosed their online activities. These ranged P011 who does almost all financial transactions online; “I pay all my bills online. I order a lot of my stuff online through Amazon. I don't think I've written a check since 2000.” To P006, who doesn’t transact online with frequency due to security considerations:

> I've always been fairly security conscious. Oh, so my typical routine, for example, I don't do online banking. I'm that guy that actually calls on the phone. I have two credit cards that are specifically used for online transactions or PayPal, because it sets up a layer between my information and any potential either intercept or hack. (P006)

Most participants reported, like P010, online activity that included online “banking, and investments, and purchases.”

Personal Guardianship Behaviors

Personal guardianship behaviors offered a small twist. It was necessary to refine the definition to include not only acts an individual performs to keep themselves secure online, but also acts they avoid taking.

When it came to personal guardianship behaviors, passwords were the most commonly reported security measure. Two-thirds of participants said that they used passwords for security. P011 said that before the breach he “used a password rotation” and after the breach he began to use “a password manager.” The majority of participants also manually monitored their online finances in some way, like P005 who said that after the breach “I checked all my banking accounts, and I was monitoring them myself.” Others report even more rigor to their behaviors using both manual monitoring and setting automatic alerts:

> I'm good. I watch stuff very closely. I'm very quick to catch anything that doesn't make any sense. … I set tighter parameters for a charge. It used to be anything above $200 I got a notice. Now I keep it at $100. If I can make it less than that, I'll do that, too. Because, again, the sooner you know something, the easier it is to stop it from actually becoming permanent. (P013)

A third of participants reported limiting the data they provide.

> I'm very hesitant to give out things like social security number, stuff like that. Too much personal data. Which I think any time somebody asks you for your full social security number, that's probably a little more than they need to know…. I was just cautious with it. I would not give it out to people unless needed. I would say that was it. (P009)

In total, participants reported the following personal guardianship behaviors: automated alerts, credit freeze, layered security, limiting information given, link validation, manual monitoring, passwords, security through obscurity, tiering data by sensitivity, using trusted networks, two-factor authentication, and VPNs. Some participants also mentioned obstacles to personal guardianship behavior including forgetfulness, inconvenience, the need to allow access to credit checks, and simply not knowing what else it is possible to do. Choosing what not to do or what not to share appears as important a component of personal guardianship behaviors as using complex passwords or two-factor authentication.

Questioning Categories: Equifax versus Facebook

Having identified categories within the Equifax case, the necessity at this point was to determine whether the categories in the first case could appropriately be applied to the second. The codes were quite similar across the two data sets; however, that is not sufficient to assure that the same categories would best serve the Facebook case data. One of the primary indicators of good qualitative research – in fact good research in any form – is to seek disconfirmation rather than confirmation (Miles et al. 2014). In the following sections, we will demonstrate the relevance of categories from the Equifax case to the Facebook case in two ways. First, we review each category and provide evidence from the Facebook cases to support each one. Second, alternative categorizations for sub-codes appearing only in the Facebook case will be discussed, as will our rationale for their inclusion in each category.

Individual Characteristics

In the Equifax case, the category individual characteristics was revised to include the constructs: “risk perception;” “self-efficacy in information security;” “work background;” and “beliefs about humanity,” which contains the sub-constructs “faith in humanity” and “suspicion of humanity.” The Facebook data did not suggest any new categories for these constructs; however, a type of risk not present in the Equifax case was perceived by some Facebook participants

Risk Perception

All participants discussed their view of risk, and participant risk perspectives covered a wide range. Some participants felt that the risk to them was low, such as P017 who said, “It was not especially risky to me, because I did not share vital data.” Some participants, like P016, felt that the risk was low before the breach, but changed that view once the breach occurred “Pretty high. Actually, very high. I feel like it's very risky.”

In addition to this general risk assessment, a few participants expressed that they no longer felt safe assuming that information was what it appeared to be online. This view is typified by the following quotation.

> I can no longer trust the news sources and the profiles that I'm looking at to be reflective of those individual people, and it makes me suspicious of absolutely everything that I see on Facebook now. So, my level of suspicion went from virtually none to now I don't trust anything that I'm seeing. And it kind of broke that innocent awareness of thinking that all of our data was protected to now realizing that these kind of social media sites like Facebook had the ability to

> damage individual lives and has consequences on a global scale that I just had not thought possible before. (P016)

Self-efficacy in Information Security (SEIS)

All participants discussed their view of SEIS, and these assessments included emotional statements such as P016 saying, “I feel incapable of protecting my information online and that's a very scary feeling.” Another perspective on SEIS presented protection as a matter of context.

> My ability to protect my information is about keeping my phone out of people's hands and having decent passwords so casual criminals or ne'er-do-wells can't mess with me. It's a little like home security in the way that I don't think it particularly is possible for me at my level to defend against an actual professional or talented or skilled or resourced attack. (P021)

Beliefs about Human Nature

All participants discussed their beliefs about human nature. The majority of participants described themselves as more suspicious of humanity. Unlike in the Equifax case, however, some people reported that this suspicion of humanity was fairly new. P024 said, “I really don't know, I'm just guessing, but my perception is that people are thinking more about themselves now than they used to. But I don't know.” He did not link this change to the breach, but rather to the political climate of our day. It is unclear whether his experience of social media in general affected his view. If so, it would align with the assertion of P023, who said, “they kind of want you to view all the bad things, and that includes view time for them, more engagement…. you start to feel worse the longer you're on there.”

Also, there were some comments that gave us pause regarding the division of beliefs about humanity into faith in humanity and suspicion of humanity. These resolved through the realization that a single comment might be coded for both sub-constructs. This dual coding occurs, for example, in this passage discussing the futility of labeling human nature as innately benevolent or selfish:

> It's still the same, because, like, people say, you know, when they argue about the idea that humans are inherently good or evil and every time people make that debate I'm like, you know that's so stupid, no, we're neither, we're both, all of it. (P023)

Other than this momentary faith/suspicion quandary, beliefs about human nature applied to the Facebook data set well.

Work Background

Unlike the Equifax case, work background rarely appeared in the Facebook case. The only meaningful instance was a reference by P017 to training on internet security provided by the Navy.

Situational Characteristics

Based on inductive analysis of the Equifax case interviews, the category of situational characteristics was included our category set. This was a general category that included the structural assurance construct as well as other situational characteristics such as mandatoriness and lack of control. In the Facebook case, several participants felt a sense of Facebook as mandatory. This was somewhat surprising, since deleting a Facebook account is not procedurally difficult. Nevertheless, largely due to social needs or obligations, several participants reported feeling trapped on Facebook. When Facebook provides one’s main communication, as it does for P019, “a lot of people in my situation have to use it for every single communication” or one’s primary social access as it is for P014 and P024 leaving can be a hardship.

> That's the thing. That's one of the reasons it's been so difficult for me to break away from Facebook. I've wanted to break from it since the breach, but some of my social groups, like my gaming group, we coordinate on Facebook, and so… But I'm having to give up, and I'm willing to give up, a lot of that convenience…. I'm going to give up the majority of social contact that I have, and it is the last form of public social contact that I have, because Twitter and everything are gone. I will have Google Hangouts with a few very close friends, and then the same very close friends are on my journal. There's no public access whatsoever. (P014)

The sense of lacking control, so commonly reported in the Equifax case, was present only for a single Facebook participant, P019, who said, “It feels very stalkerish. It feels very much vulnerable, like Facebook has given binoculars to somebody in the world into my window and I don't have any control over it.” Only one participant touched upon structural assurance in any form, and that was without any expectation that such assurances would come to pass. P023 summarized the situation succinctly if profanely “the government is fucking inept because they're too old to understand [Facebook], and they probably would be bribed out even if they did.”

In short, the primary situational characteristic to affect participants who included in the Facebook case was mandatoriness. Despite the fact that Facebook is an optional service in the sense that a user is not enrolled automatically and can delete their account, users rely on Facebook for social support, communication, and other activities central to their lives.

Data Characteristics

It became clear in the Equifax case that some users consider their data's value and sensitivity. Half the participants in that case argued that data characteristics were important to the calculus of security. In the Facebook case, two-thirds of participants discussed their data. Users reported not realizing the risks of aggregate data.

> "If everyone's talking about politics, I'm like, "Well, everybody's talking about politics, so this information's probably not really needed since it's just like the general noise….there were so many people [posting their political opinions], that we can all just do it willy-nilly almost, and not have to worry about anybody being interested in that because already is, everybody's doing it….Of course, then afterwards, I was like that's exactly why it was vulnerable." (P015)

P015 went on to say "I guess I really underestimated what value that data might have to others." P016 said "the breach kind of— it increased my awareness of how important that information was, if that makes sense." Many users discovered through the breach that they had much more at stake than they had thought:

> I thought they basically had access to my posts, people I interacted with, and again like any cute cat pictures or anything that I put up. I guess I felt that that data was fine, but that was also data that I was willing to share with other people anyway. A lot of that comes from a place of ignorance for me, where I just didn't realize how much... Again, if I had known how much they were gathering, I would never have signed up for it anyway. (P014)

The main theme of these all these discussions centered on the difficulty for users to determine what data was being collected and to assess the value of their individual data as part of a larger aggregation.

Breach

This construct was present in our original model as “breach notification.” It was modified to include “breach awareness” in order to overcome obstacles to participant recruitment. This data in the Facebook case regarding breaches was quite similar to the data in the Equifax case. Participants reported that breach awareness triggered changes to their perspectives. P014 said, “I never took [online security] seriously before the Facebook thing, and now I take it ultra-seriously.” Also as with the Equifax case, Facebook participants reported that combinations of breaches caused changes in protective behavior. P018 says “it’s kind of hard because I’m not sure which came first Facebook or Equifax but the combination of both of those things [caused me to change my protective behaviors].”

In addition to the findings from the Equifax case, in our analysis of the Facebook data we discovered that the method of breach notification can be quite important to how the user feels about the company Facebook notified users of the breach through a statement of their Facebook news feed. This notification disappeared once the user interacted with it. This lack of permanence struck some as questionable.

> I don't have anything in my email about it. I don't have anything in my like Facebook messenger…. There's, like, so it's obviously gone from my news feed, so really nothing that I can find immediately that like this even happened. Yeah. It’s just …there’s nothing. It feels a little…shady. (P003)

External Guardianship Beliefs

The majority of participants in the Equifax case did not report holding external guardianship beliefs about Equifax prior to the breach, but after the breach, users developed largely negative views of Equifax as a data guardian. The same dynamic did not arise in the Facebook case. Unlike Equifax, which collects user data from third parties, Facebook gathers data directly from their users. Thus, it was no surprise to find that all participants were aware of Facebook, even prior to the data breach. Instead, the surprising revelation during data analysis was the view of Facebook as a product provider with no guardianship responsibilities, despite the amount of data in their possession. Discussing her view prior to the breach, P014 said, “In the same way that I would download a computer game, and the download goes kind of the same way, and then I play the game, and then I can take it off the computer when I want to. I felt like [social media platforms] were much more basic structures than they are.” Some users changed their view once the data breach occurred, but for others this perception extended past the breach into present day. Post-breach, P022 said, “I don't think Facebook's a guardian of my data.” P021 said. “I assumed Facebook isn't a meaningful guardian of my data.” Even the users who felt that Facebook should be guardians of user data, did not express any belief that they would act in that way. P020 said, “no one else [but me] is looking out for my data.”

User Online Routine

User online routine is composed of the sub-constructs: “online activity” and “personal guardianship behaviors.” Our definition of online activity has remained stable: actions a user takes online without a security motive (Yar 2005). Our definition of personal guardianship behaviors was revised slightly during analysis of the Equifax case to include both acts an individual performs to keep themselves secure online, and also acts they avoid taking. The definition of these constructs remained stable in our analysis of the Facebook data. However, there was a major shift in the meaningfulness of online activity as a measure of breach impact.

Online Activity

In the Equifax case, users did not change their online financial activities as a result of the breach, possibly due to the fact that users lacked the ability to leave Equifax or remove their data from Equifax's control. By contrast, many participants reported changes to their online social media activities after the Facebook breach. All participants willingly disclosed their online activities. These ranged from P024 who uses only Facebook: "It's pretty much Facebook and that's it, really." To P006, who has accounts on "Instagram, Twitter, Snapchat, and Patreon" as well as Facebook. Most participants reported using Facebook less after the breach. P018 said simply, "I get on Facebook less."

A third of participants reported leaving or planning to leave Facebook. On the subject of leaving Facebook, P014 said: "At this point, one of the reasons I'm leaving Facebook is because I have become increasingly aware of the data that they're continuing to gather, despite reassurances that everything is fine." In addition, half of the participants reported reduced Facebook use. Some participants also reported uninstalling the Facebook app in an effort to gain distance from the site. Oddly, some users reported leaving other social media, but remaining on Facebook. P014 says, "I had a Twitter account at the time. I'd started an Instagram account. I locked both of those down and deleted them immediately [after the breach].” P019, who is reliant on Facebook for their primary communication says, “I stopped interacting on Facebook as often,” but they did not leave the site.

Personal Guardianship Behaviors

When it came to personal guardianship behaviors, in the Facebook case, passwords were surpassed by two other personal guardianship behaviors. Privacy controls were the most commonly reported security measure in the Facebook case. All participants said that they used privacy controls for security. The majority of participants also reported limiting the information they provided, such as P017 who said, “So my personal mitigation for [risk] was to give Facebook less of my data.” P003 wondered if these restrictions “would defeat the purpose of social media.” Nevertheless, she and most other participants have made use of these data limitation techniques to protect themselves and their social media data online.

Cross-Case Analysis

Multi-case studies allow the emergence of common conclusions which can provide evidence of transferability as well as indications as to the boundaries of a chosen theory (Yin 2018). We chose two cases with similar characteristics, but with enough differences that we hoped comparison of the two cases would be illumination. Between our cases, there were many similarities in the themes. In fact, at the categorical level, the cases supported one another.

Summary

This chapter provided a complete description of our data analysis. In it we also presented the six theoretical categories found in the Equifax and Facebook cases. These were individual characteristics, situational characteristics, data characteristics, breach, external guardianship, and user online routine. The ways in which aspects of these categories differed or remained stable between cases was demonstrated both through explanatory text and participant quotations. Finally, a comparison of the two cases was provided. In the next chapter, we will discuss our findings regarding how these theoretical categories relate to our research questions and present propositions based on our findings.

Chapter Five: Findings

Introduction

The goal of this study has been to elaborate on existing Routine Activity Theory research to answer the research questions:1) How do individuals determine their personal online routines given that they are reliant for data protection on external guardians over whom they have little or no control? and 2) How does awareness of a data breach impact this process? In Chapter Four, we described our analysis of participant interview transcripts and identified six theoretical categories arising from this analysis. In this chapter, we will show how these categories relate to our research questions, discussing how the categories affect the process by which users determine their online routines in an environment where data breaches are common and users must rely on external guardians over which they have little or no control. Finally, we will offer propositions based on these findings to help guide future research.

Findings

At the outset of this research project, we reviewed relevant research in the IS security field and identified a promising theory from criminology to assist in our investigation. From these sources, we weighed and selected constructs that we deemed likely to play a role in users' process. Next, we developed an interview script based on our tentative model of the process by which users make decisions about their online routines. Given relative paucity of research into this specific topic, we chose a qualitative research method due to its flexibility and robustness. By gathering a rich qualitative data set, we could find support for *a priori* constructs and retain the ability to uncover new constructs of relevance (Miles et al. 2014). In the process of this research, we found six theoretical categories which hold relevance for users creating and continuing their online routines. This chapter is devoted to the discussion how our inquiry answered our primary research questions. We will take a step back from the constructs and sub-constructs discussed in prior chapters in order to give a high-level view of users' process as it develops and changes over time.

Research Question 1

How do individuals determine their personal online routines given that they are reliant for data protection on external guardians over whom they have little or no control?

Determining Online Routines

Online routines are, exactly that, routines: sequences of actions performed habitually (Visetelly 1936). Individual users develop and modify those routines over time, based their needs, personal preferences, and many other factors (Cohen & Felson 1979 and Yar 2005). In answering the question of how users select online routines given their reliance on external guardians, we have found that the individuality of users plays a central role. To be an individual is to have a unique mosaic of characteristics including one's personality, aptitude, experiences, and more. When we present individual characteristics as a category relevant to the process by which users develop and maintain online routines, we refer to that uniqueness. Through our analysis of interview data, we identified specific individual characteristics that our participants described as affecting their decision-making online: risk perception, SEIS, beliefs about human nature, and work background. These guide participants' perceptions, beliefs, and behaviors. But we also found that characteristics outside the individual affected participants' decision-making process regarding their online routines.

Our analysis revealed that user's perceptions the characteristics of a situation came into play when determining online routines These situational characteristics are not innate to the user but, instead, relate to their view of the interactions taking place between themselves, the sites they visit, and the online environment. Structural assurance mechanisms, such as regulations, are an example of such a characteristic. Participants reported that their understanding of these situational characteristics and the options available to them as a result influenced their online routines.

In addition to characteristics of the individual and of the situation, users reported that their perceptions of data characteristics also played a part in choices about what to do and how to do it online. The way users see data that they generate, how that data is collected and combined by third parties, and the value of that data to potential attackers' forms part of the calculus they use to determine their online routines.

Ultimately, users consider each of these characteristics – individual, situational, and data – when determining their online routines. Who a person is, what they perceive the nature and structure of online interactions to be, and their views about data all interact to influence their choices regarding online routines. But, what of external guardians? In undertaking this research, we sought to uncover how reliance on external guardians over whom they have little or no control affected the online routines of users. In the following section, we describe our findings on this matter.

Reliance on External Guardians

The relationship between external guardianship beliefs and users' online routines is more complex that we initially expected. Our analysis shows that users often do not think about organizations that are responsible for their data until something bad happens, like a data breach. When users do consider organizations that are in possession of their data, they don't necessarily see those organizations as guardians. In fact, many users seem to perceive these relationships as almost adversarial – a struggle between those organizations that want data and users who want to access services without putting themselves or their data at risk.

In the Equifax case, external guardianship beliefs were not meaningfully present prior to the breach. By this we mean that many users reported that they simply did not think about Equifax having their data and therefore being responsible for its protection. Users did not consider Equifax as a data guardian, because they did not think about Equifax's role in a user's online presence. This view was exemplified most often by the phrase, "I did not think about Equifax at all." Three quarters of participants in the Equifax case exhibited this view, including some individuals with strong positive feelings of SEIS and/or professional security backgrounds. It is not the opinion of the researchers that users were to blame for not attending to the security posture of Equifax.

At first, we expected that this phenomenon would be limited to participants in the Equifax case. The relationship between Equifax and its users is markedly different from the relationship of Facebook to its users. Equifax collects data on its users primarily from third parties, and its customers are not the users considered by our study but rather financial and other organizations seeking information about those users for various purposes. Perhaps, users didn’t consider Equifax as a data guardian, because they didn’t know Equifax had their data in the first place. This possibility was supported by participant statements such as:

> I didn't really think about them much. They're just a credit reporting agency is the way I saw them. I don't think I even considered that they stored our data online, which I guess they would have to for all the banks and, you know, loan application folks to get your information. (P005)

Surprisingly, though, even in the Facebook case, several users reported that they did not view Facebook as a guardian of their data. Rather they saw Facebook as either a product supplier, a semi-public venue, or an actively exploitative actor. These views are reflected, respectively, by the following participant quotations.

> I figured that all social media platforms were doing their one thing, and that was the thing they were doing, and they were all basically doing it the same way. In the same way that I would download a computer game, and the download goes kind of the same way, and then I play the game, and then I can take it off the computer when I want to. I felt like they were much more basic structures than they are. (P014)

> Oh, I don't think Facebook's a guardian of my data…. I think of them like a bulletin board in a coffee house. It's a place where I can put things. I can control that the people in that coffee house are the ones seeing it, but somebody could wander in, you know? (P022)

> A data guardian? I have no faith in Facebook as a data guardian whatsoever. When a company amasses billions of dollars in such a short amount of time, the

> idea of them at all having any kind of perspective towards the best interest of the consumer is laughable, in my opinion. (P023)

Strong negative emotional charge was evident in the responses of participants with this view. Rather than relying Facebook or Equifax as external guardians, many participants described feeling reliant on their own individual characteristics, situational characteristics, or data characteristics to protect them from harm online.

Participants also spoke of the limits of these protections. Some users perceived online risk as insurmountable for anyone, such as P006 who, as mentioned earlier, views the security of online exchanges as "nightmarishly awful in all cases." Other participants feared, rather, that their own lack of skill made them individually powerless where different person might be capable of protect their own data. One user spoke feelingly of her reliance on security through obscurity:

> I mean there's a lot of information out there, and so I just sort of picture my information as being one of many chunks of data just kind of floating out in the world, and people who try to catch that data are maybe using nets and maybe they catch some of my data and maybe they catch some of other people's data. I just kind of honestly for a very long time I've been counting on my data not being particularly useful to people and that that keeps me safe. (P001)

When a user felt that they had done all they could to protect themselves, a sense of fear, anger, or hopelessness at times appeared.

Negative emotions were also evident in the interview of those participants who *did* view Equifax and/or Facebook as external guardians of their data. Participants argued that it is reasonable to assume that organizations in possession of one's data have a duty of care which they take seriously and enact responsibly. Users reported that they developed their online routines based on the assumption that firms were willing and able to fulfill their duty to protect the data in their possession. For these users, this belief affected both their choice of online activities and the extent to which they adopted personal protective behaviors, in addition to the individual, situational, and data characteristics that influenced the online routine of all users in our study.

Research Question 2

How does awareness of a data breach impact this process?

Breaches and External Guardianship Beliefs

Unsurprisingly, in many instances, users reported that breaches affected their external guardianship beliefs. As mentioned in the previous section, without a breach, users might not even think about external guardians or might not consider the guardianship element of a relationship between themselves and an organization. In the Equifax case, the majority of users never considered Equifax's guardianship before the breach occurred. However, our findings show that after users become aware of a breach, they reassess. The majority of participants in the Equifax case reported a negative view of Equifax's guardianship since the breach. P004 described this succinctly, "I went from not having a perception, necessarily, to having a perception that they suck." P007 said "Oh, I don't think Equifax can provide protection for the data. I don't think they really offered a solution." In the Facebook case, many users reported profound changes to their beliefs. P016 describes her shifted view:

> I very much kind of lumped Facebook and Google and a lot of these major organizations into the same category…as this progressive new age of companies

> that were willing to go the extra distance to make sure that they protected my security and that they had my own best interests at heart because they kind of "got it". … And I don't feel that now.

It was not always true that awareness of a data breach changed users' views of an organization's guardianship. One quarter of participants in the Facebook case did not report a change to their external guardianship beliefs after the breach. However, this generally occurred when the user in question already held a negative view of Facebook. P022 explained beginning with the assumption that Facebook "cannot and do not and would not" protect her data. Thus, news of the Facebook breach left her feeling "vindicated" in her view, rather than triggering an alteration to that belief. Nevertheless, many users reported that awareness of a data breach caused them to develop more negative beliefs about an organization's guardianship. In addition to these findings, analysis revealed another unexpected aspect to users' revisions of external guardianship beliefs: expectations of improvement.

Many participants across both cases said that they expected external guardianship at the breached organization to improve for a time after a breach announcement. Some thought the changes to security would be superficial, while others expected substantive improvements, but nevertheless many participants reported the belief that both Facebook and Equifax would devote considerable resources, in effect, to locking the barn door now that the horse was free. Users with this view did not demonstrate positive sentiment toward these external guardians, possibly due to the fact that users did not attribute this improved performance to benevolence on the part of the firms. These participants argued, rather, that fear of lawsuits or falling stock prices drove a belated focus on security.

Analysis revealed one additional insight regarding the relationship between breaches and external guardianship beliefs. The manner in which an organization handles a data breach announcement matters to users. When an organization delays, minimizes, or attempts to deflect blame for the breach back on the individual, users express negative beliefs about the external guardians.

Breaches and Characteristic Categories

As reported in our discussion of research question 1, users consider individual, situational, and data characteristics when determining their online routines. After learning of a data breach, users reported changes to their perceptions of these characteristics. While, in general, it our intention in this chapter to provide a high-level view, our findings on the nature of these changes yielded some information regarding the effect of breach awareness on specific individual characteristics, which we feel is best approached by a brief discussion of two constructs within the category of individual characteristics. Our findings show that, for our participants, breach awareness affected risk perception and SEIS. This was particularly evident in the responses of users who reported feeling fairly secure prior to the breach. In the Facebook case, half of all users reported that the breach increased their sense of risk. Illustrating this, P018 said, “I thought it was less risky [before the breach] than I think it is now.” In the Equifax case a smaller proportion of users reported an increase in risk perception, though the shift was present for some. This difference may be result from the fact, mentioned previously, that many users did not hold conscious views about Equifax as a guardian prior to notification of the breach. Nevertheless, some participants in the Equifax case did report this view. P10 said that before the Equifax breach occurred, he thought sharing data with financial companies online was: “Not very risky. I have a basic assumption that they know what they're doing.” After the breach, he says “If it happens once it can happen again.” This finding aligns with prior work showing that adverse events result in changes to user perceptions (Rhee et al. 2009).

When users already viewed the situation as risky, awareness of a data breach understandably reinforced that risk assessment rather than causing that perception to change. Across both cases, most users who reported no change to their risk perception stated that the breach confirmed their risk assessment. For example, P013, a participant in the Equifax case, said that her view of risk didn’t change after the breach, because the breach provided support for her preexisting view: “Didn't really change it. I think it's all a racket.” Similarly, P017, a participant in the Facebook case, said “I would say [the breach] was in the confirmation category.” From this evidence, we determine that breach awareness affects the individual characteristic of risk perception, except where a breach occurrence would confirm a user’s preexisting view.

Another individual characteristic, SEIS, was affected by breach awareness. This finding is in keeping with prior research that states security breach incidents affect SEIS (Rhee et al. 2009). In the Equifax case, half of all participants described changes to their SEIS after notification of the breach. For example, P012 said the breach “made me doubt slightly my ability to protect [my information].” This was effect was evident across both cases, but in the Facebook case, response reflecting this position constituted a majority of all participants.

> So it lowered my confidence, kinda like what we’ve been talking about. I realized that some of it is just out of control no matter how careful I am. Like, we’re all

> connected on social media, so all it takes is one person in the web to take a wrong step and then everyone's data is just out there. So, I—as far as what I can do about it—I can not have friends, but that sort of defines social media. (P003)

Participants in the Facebook breach case also used more emotive language when discussing this shift in view. P016 said that since the Facebook breach "I feel incapable of protecting my information online, and that's a very scary feeling."

In addition to the impact of breach awareness of user's individual characteristics, user's perceptions of situational characteristics also changed after users became aware of a data breach. Participants reported that they expected their online routines to be protected in the same way that their offline routines are governed by laws and norms. They expected systems to be in place to protect routines that they see as normal and commonplace. In describing the discovery that data breaches can occur without external guardians experiencing any adverse consequences users described feeling angry and betrayed.

> It kind of feels like emotional blackmail kind of thing. Like, we're not going to protect your data but if you don't use us then your kind of cut off from your family, because they all use Facebook and they're not going to quit. (P003)

Breach awareness also altered the way users perceived their data. The fact that they data had been stolen or sold seemed to result in a revision of participant's perspective about what data these organizations hold and what that data is worth. After the becoming aware of the breach and its implications, many participants reported reassessing their perception of data characteristics.

In sum, the categories of individual, situational, and data characteristics affect users' online routines. Awareness of data breaches can result in changes to users' perceptions of these categories. Next, we will address how breaches affect online routines.

Breaches and Online Routines

Individual users develop and modify their online routines over time (Yar 2005). Across both cases many participants reported that, when they became aware of a data breach, they changed their routines in some way.

User online routines are comprised of two sub-constructs: online activity and personal guardianship behaviors (Yar 2005 and Leukfeldt & Yar 2016). In the Facebook case, many users reported substantial, meaningful changes to their online activities after the breach. P016 said, "honestly as a whole, it decreased my Facebook use and made me a lot more aware of any posts that I was making and what personal information somebody could gather from that." P018 reported, "I think I get on Facebook less." P019 no longer comments the way they used to, "I don't really interact because I don't want people seeing me."

By contrast, in the Equifax case, users generally reported no changes to their online activity. This lack of alteration reflects participants' statements about feeling a lack of control when it came to their financial routines. Participants seem to see no way to extract their data from Equifax, and thus continue with their online activities unaltered. Our analysis suggests that when users don't feel that they can control an external guardian's possession or management of their data, they tend to maintain their online activity without alteration.

In both cases, most users reporting changing many of their personal guardianship behaviors after becoming aware of a breach. Equifax users such as P004 reported now "using strong passwords and different passwords for every account." P006 said, "I have changed the way I do passwords." P009 says, "Setting up the alerts, of course, was a thing that gave me more comfort in the transaction part of it." P013 says she now avoids purchasing from websites she doesn't know "I'd rather pay a few more dollars just to go to someplace that I know the reputation is there." Facebook participants also changed their behaviors. P003 now restricts what information she provides: "I just don't give any more information than I absolutely have to." P017 no longer relies on Facebook for security:

> I no longer use the Facebook single sign-on, which there were a couple of accounts that I did use it before. That's not true. There is one account that I still have to use the Facebook single sign-on, and it grates upon me… That's exactly right. Yeah, my library application, the web app, I have logged once with Facebook. When I'm like, okay, delete that account, log in as new account, it says nope, we actually already have a record at this address, this email address. It will not let me log in as my email address. It makes me use Facebook.

P017 resents the library presenting an obstacle to his chosen protective behaviors.

In both cases, the majority of users reported increasing their personal guardianship behaviors in one or more ways.

After awareness of a breach, many users enact protective measures, but those measures have an upper limit. Users can only add the personal guardianship behaviors that they know exist and are capable of performing. This upper limit of self-protection left some participants feeling unmitigated vulnerability. As an exemplar of this view, P001 said, “I just sort of picture [data breaches] as like car accidents. They happen sometimes. They don’t happen sometimes. I don’t feel like I have a lot of control over the situation.” Interestingly, data breaches prompted changes online activities and personal guardianship behaviors not only to the online routines associated with the breached organization, but also in entirely unrelated aspects of online life. One might expect such an occurrence if users made sweeping changes across all aspects of their online routine, and that did occur. Some users changed all their passwords everywhere, for example. But, paradoxically, some users reported making changes to their online activity in ways that affected their routine with the exclusion of the breached organization. This was evident in the case of Facebook participants. Several participants in this case reported leaving other unbreached social media sites, such as Twitter, Tumblr, or Instagram, but retaining their Facebook accounts. When asked about these decisions, users discussed viewing Facebook as a mandatory part of their lives. This was true chiefly for participants relying on Facebook for social connection to friends or family with whom they had limited access through other means. It is evident that, whether due to a literal inability to extract themselves from an online relationship, such as users experience in the case of Equifax, or a practical inability to sever an online relationship, as in the case of some Facebook users, some users continue behaviors they see as risky, because they not see an alternative to the routines they currently enact.

Finally, participants explained that not all breaches have equal effects. The larger the breach, the more valuable the data breached, and the more breaches of which a user is aware, the more dramatic the changes users are motivated to make to their online routines.

Propositions

In the following section, we put forward a set of propositions to build upon our findings in future research. Herein, we articulate our propositions and discuss how they align with or diverge from prior understanding.

Proposition 1

Across both cases, individual characteristics of users affected user's online routines. Specifically, users' risk perception, self-efficacy in information security, beliefs about human nature, and work background all played a part in both user's online activity and personal guardianship behaviors. This leads to our first proposition:

> *P1: Users' individual characteristics – including risk perception, self-efficacy in information security, beliefs about human nature, and work background – influence users' online routines.*

Proposition 1 aligns with existing work in the IS security field stating that users make decisions about security based on their assessment of risks (Liang & Xue 2010) and extent to which their SEIS enables them to avoid that risk (Herath et al. 2014). It also integrates well with findings from IS research on the mechanisms of trust formation stating that in order for trust to occur, users must also have a willingness to depend on others (McKnight and Chervany 2001b). Prior research has also found aspects of personal experience relevant to decision making (Liang & Xue 2009 and Wang et al. 2017). Thus, the relevance of work background is in good alignment with existing understanding. Given the ample support in prior research showing that individual characteristics significantly affect security perceptions (Wright & Marett 2010), decision-making (Dinev & Hu 2007), and behaviors (Rhee et al. 2009), we are unsurprised to find sufficient evidence to put forward this proposition.

Proposition 2

Across both cases, user perceptions of situational characteristics affected user's online routines. Relevant situational characteristics included structural assurance as well as perceptions of mandatoriness and lack of control. This leads to our second proposition:

> *P2: Situational characteristics, including structural assurance and perceptions of mandatoriness and lack of control, influence users' online routines.*

Proposition 2 builds on work in the IS field of trust research, which states that users consider situational characteristics such as structural assurance when choosing which behaviors and technologies to adopt (McKnight & Chervany 2000, McKnight and Chervany 2001b, McKnight et al. 2011). We believe that applying constructs from the trust literature to IS security research will provide a fruitful avenue for future research. Mandatoriness has also been found in prior IS research to affect the emotions of technology adopters (Beaudry and Pinseonneault 2010). However, the construct has not been studied in much depth in the context of user's determination of online routines. We suggest that, going forward, researchers in this area would do well to consider the effects of both functional and perceived mandatoriness on users' online routines.

In IS research on privacy, control or lack thereof has been found relevant to users' decision making around e-commerce (Malhotra 2004). Users also consider their level on control when adopting new technologies (Crossley & Posey 2017). Our findings align with this prior work and offer another research area where user's perceptions of control impact behavior.

Considering situational characteristics in future research on users' development of online routines should provide useful insights going forward.

Proposition 3

Our findings show that user's perceptions of data characteristics play a part in user's determination of online routines. The value users place on the data that they generate, their perceptions of organization's data collection and aggregation, and the usefulness of that data to potential attackers are all part of user calculus in determining their online routines. This leads to our third proposition:

P3: Data characteristics influence users' online routines.

Prior RAT research focused on guardians and offenders includes target value as a construct that affects the decision making of both guardians and offenders (Cavusoglu et al. 2008 and Png & Wang 2009). Yet, we can find no prior IS security research that considers, in detail, users' assessment of the value of their data as a potential target for comprise. Further examination of how users assess the value of their data and how that assessment influences their development of online routines could provide valuable insight into user behavior online.

Proposition 4

Our research supports the idea that when users 1) possess external guardianship beliefs about an organization and 2) perceive an organization to be a data guardian, their external guardianship beliefs affect their decisions regarding online routines. This leads to our fourth proposition:

P4: Users' external guardianship beliefs affect users' online routines.

Researchers using RAT have drawn a distinction between a routine online activity and an individual's personal guardianship behaviors (Leukfeldt & Yar 2016). Prior IS research has found that beliefs about external guardianship affect personal guardianship behaviors (Rhee at al. 2005). Our research also found support for the effect of external guardianship beliefs on online activity, a finding not present in other IS security research. Analysis revealed considerable complexity around the formation external guardianship beliefs and their impact on users' online routines, which provides a broad and fertile area for future study.

Proposition 5

Across both cases, after becoming aware of a data breach, users reported changes to their individual characteristics, with the most frequently affected characteristics being user's risk perception and SEIS. This leads to our fifth proposition:

P5: Data breach awareness affects users' individual characteristics.

Prior IS security research supports the view that users' perceptions and beliefs change when adverse events occur (Rhee et al. 2009). Given that a data breach represents an adverse event, we are in alignment with existing research. We provide this proposition as an additional context to which existing understanding can be applied.

Proposition 6

Our analysis shows that user's perceptions of situational characteristics changed after users became aware of a data breach. In both cases, users reported that they expected systems to be in place to protect their online routines. Awareness of a data breach led users to conclude that no such sufficient protections exist. This finding drives our sixth proposition:

> *P6: Data breach awareness affects users' perception of situational characteristics.*

As in our discussion of proposition 5, we note that prior IS security research supports the view that users' perceptions and beliefs change when adverse events occur (Rhee et al. 2009). IS researchers have found that data breaches result changes to customer behavior and can lead to spillover effects that can impact entire industries (Culnan & Williams 2009). Further examination of how data breaches affect users' perception of situational characteristics may yield additional discoveries.

Proposition 7

Our participants report that data breaches trigger reassessment of the characteristics of their data. After becoming aware of a data breach, users across both cases reported re-evaluating the value of their data to organizations and offenders. This leads to our seventh proposition:

> *P7: Data breach awareness affects users' perception of data characteristics.*

Though IS researchers have found that users exercise personal guardianship selectively based on their perceptions of the importance of data and its likely security (Chen & Zahedi 2016), at present, we have uncovered no prior work in the IS field explicitly studying the relationship between data breaches and user's reassessment of data characteristics. Prior research does show that users choose what to share online based on their perceptions of data value (Tow et al. 2010). Thus, we suggest that future study of this proposition could form a foundation enabling meaningful contributions to understanding user's decision-making online.

Proposition 8

Across both cases, users reported that data breaches affected their external guardianship beliefs. In the Equifax case, many users formed their initial external guardianship beliefs about the firm for the first time *after* notification of the breach. In the Facebook case, users were more likely to report changes to, rather than instantiation of, guardianship beliefs. Nevertheless, in both cases, data breach awareness played a role in user's external guardianship beliefs. Thus, we propose:

P8: Data breach awareness affects users' external guardianship beliefs.

Though IS security research in this area has generally focused on preventing data breaches, prior IS research in the realm of service recovery foreshadowed our findings regarding a relationship between data breach awareness and user's external guardianship beliefs, having shown effects on user continuance intentions occur when organizations experience a data breach (Goode et al. 2017). However, given that this research focused solely on means by which organizations could mitigate adverse outcomes post-breach, there remains a wide field of investigation available related to this proposition.

Proposition 9

User online routines are composed of a user's "online activity" and "personal guardianship behaviors" (Yar 2005). In the Facebook case, many users reported changes to their online activities after the breach, while in the case of Equifax, users generally did not report a change to their online activity. Across both cases participants reported that, when they became aware of a data breach, they changed their personal guardianship behaviors. Thus, we propose:

P9: Data breach awareness affects users' online routines.

We have found little existing research that examines this relationship explicitly and centrally in the context of individual users outside a work context. Future research is necessary to identify the boundary conditions that govern when a user changes their online activity *and* personal guardianship behaviors, as compared to those contexts in which users' change their personal guardianship behaviors alone, and to identify cases of which users make no changes. Longitudinal studies capable of establishing causation would be of particular help building understanding of relationship described by this proposition. In short, we believe that the dynamic between data breach awareness and users' online routines, in all its variations, warrants extensive scrutiny.

Summary

In this chapter, we discussed how our findings answer our two research questions, introduced propositions based on these findings and related those propositions to prior research. In our next chapter, we will present our conclusions including contributions to theory and practice, study limitations, and directions for future research.

Chapter Six: Conclusions

Introduction

This chapter is presented in three sections: contributions to theory and practice, directions for future research, and study limitations. The contribution section relates the findings and propositions in the chapter five to existing literature. In areas that prior literature fails to cover or where our findings diverge those of prior works, we articulate how the results of our study fit with the extant nomological network.

The goal of our study has been to use Routine Activity Theory to illuminate the process by which users outside organizations determine their online routines, how the process is affected by awareness of a data breach, and in what manner user reliance on external guardians over which they have little to no control affected this process.

At the end of our research we understand this process somewhat better. We know now that user's online routines are affected by individual, situational, and data characteristics. We also now understand that there exist relationships between these characteristics and users' beliefs about external guardians, and that these relationships are complex and multi-faceted. We have also seen that users' awareness of external guardianship of their data is affected by whether users interact with a guardian actively or passively through a third party. We found support for a relationship between users' external guardianship beliefs and online routines, but it is also clear from our analysis that beliefs about guardianship are not the only factors that users consider with determining these routines and deciding whether to alter their online routines after a breach occurs.

Users change their beliefs about themselves, their online environment, their data, and their external guardians when breaches occur. Breaches can act as trigger moments resulting in widespread changes to perceptions, beliefs, and behaviors. Additionally, we have learned that users react to data breaches even when their data is not directly impacted, as was shown by users in our Facebook case, who were aware of but not targets of that data compromise. Also, we have seen that the manner in which data breaches are announced and the timeliness with which affected users are notified has an effect on users' external guardianship beliefs. It is our earnest hope that work has made valuable contributions to understanding the process by which users determine their online routines, in light of their reliance on external guardians, and how this process is affected by awareness of a data breach. In the next section, we outline specific contributions to the literature present in this dissertation.

Contributions

In this section, we present our contributions to theory first and then contributions to practice.

Theory

This research extends our current knowledge in the IS security socio-behavioral research stream which positions security within the realm of human decision making (Hua & Bapna 2013). Our first contribution to theory is identification of three theoretical categories that affect user's online routines: individual characteristics, situational characteristics, and data characteristics. Versions of these categories have been employed within IS literature in the past. Prior IS security research has shown that individual characteristics significantly affect security perceptions (Wright & Marett 2010), decision-making (Dinev & Hu 2007), and behaviors (Rhee et al. 2009). Prior IS research on trust states that users consider situational characteristics such as structural assurance when choosing which behaviors and technologies to adopt (McKnight & Chervany 2000, McKnight and Chervany 2001b, McKnight et al. 2011). To a limited extent, prior RAT research includes data value as a construct that affects the decision making of both guardians and offenders (Cavusoglu et al. 2008 and Png & Wang 2009). Our work extends these findings. Our contribution here lies in the application of these categories to users' determination of online routines.

Our second theoretical contribution elaborates on RAT. In our work, we introduced partitioning of the guardianship construct into a binary. Prior RAT research on the role of guardianship in online crime considers physical, social, technological, and national guardianship constructs in addition to the personal guardianship construct (Yar 2005, Bossler & Holt 2009, Williams 2015, and Leukfeldt & Yar 2016). These affect the guardianship an organization provides, but the mechanisms such constructs represent are not subject to separate assessment and alteration by users. Thus, we have argued that, when studying the target/guardian dyad, a simple division between personal guardianship and external guardianship is most useful and appropriate. The reduction of guardianship to this binary enabled us to gain insight into users' beliefs about external guardians.

As anticipated by prior works, we found that users do not always know which organizations hold their data or what forms of guardianship those organizations employ (Schneider 2009). We built on that understanding through the discovery that the development of external guardianship beliefs can be triggered by awareness of a breach. Our research also presents the new but logical finding that when a user holds a negative view of an external guardian prior to a breach, their external guardianship beliefs are unchanged by the breach announcement. We also discovered that users perceive mandatoriness to be a relative concept and include both a literal inability to remove themselves from an online relationship as well as a practical inability to sever an online relationship, when describing online routines that they must continue to perform.

We found support for a relationship between external guardianship beliefs and online routine, a relationship not adequately covered by prior IS security research. Our evidence shows that external guardianship beliefs influence users' adoption of personal protective behaviors and to some extent online activity as well.

Though existing research has already shown that data breaches affect consumers' perception of firms and their continuance intentions (Goode et al. 2017), our research confirms that data breach awareness affects online routines. We uncovered complexity in the nature of this effect that highlights the need for further research to identify the conditions that govern when a user changes their online activity *and* personal guardianship behaviors, when users change personal guardianship behaviors alone, and under what circumstances users make no changes. Furthermore, our study shows that data breach awareness affects individual, situational, and data characteristics, triggering revisions to each with the following caveat: when awareness of a data breach supported rather than challenged a perception of a characteristic that characteristic did not change.

Practice

This research also has implications for practitioners. Firstly, our research indicates that when making breach announcements organizations should act promptly, take responsibility for the security lapse, and clearly convey what improvements the firm will undertake to ameliorate any negative effects and prevent future breaches. Secondly, we have learned that breaches serve as trigger moments for the adoption of improved personal guardianship behaviors. This finding has relevance for firms offering protective measures, security-oriented non-profits, and government agencies charged with improving the online safety. In the period after a noteworthy breach or series of breaches, users are likely to seek out new methods of self-protection. Firms with products or services enabling such self-protection should consider marketing strategies in alignment with this finding. In turn, government agencies and security-oriented non-profits should consider the interval after a noteworthy breach or series of breaches opportune for the release of relevant cybersecurity training materials.

Lastly, we wish to highlight for policy makers the expectations users expressed regarding structural assurances. Participants reported a presumption that structural assurances in the form of regulations and opportunities for civil suits applied when their data was held by an organization and comprised during a data breach experienced by that organization. This assumption affected users' online routines. When expectation and reality are out of alignment on matters of safety, a dangerous ambiguity is formed. Policy makers should consider the benefit of alterations to our laws and regulations to bring them into alignment with user expectations or else assess methods to improve users' understanding of the laws and regulations as they stand, in order to resolve this area of misunderstanding.

Directions for Future Research

In chapter five, we innumerate nine propositions, the further study of which we feel would enable scholars to better predict user decision-making in this period of frequent data breaches. In addition to these avenues for future research, we add here one final area for exploration.

The Missing Motivated Offender

In our research, we have examined the relationship between the user and the organization. To do this we employed Routine Activity Theory to shed light on the dynamics present in the interaction between these two actors. As a conscious decision, we omitted from our study and our interview questions the third actor present in this criminology theory: the motivated offender. Nevertheless, the motivated offender peaked from the edges of our data. This is not surprising. If we had researched the interaction between 7-11 owners and customers who had been present when the 7-11 was robbed, we would reasonably have expected the occasional mention of the masked gunman. What was surprising was that in all our interviews not one negative word was said about the attackers who took the data. Offenders were described not only in neutral terms, almost like the weather, but also with positive diction. They are "savvy," "resourceful," and "creative." These are not the kind of language we expected to hear in relation to the villains of the piece. This creates a point of interest. Our research indicates that users, at present, place blame for breaches on the organization breached. This is a marked difference from offline interactions where individuals usually place the blame for stolen material on the robber. We consider this puzzling revelation worth investigation.

Limitations

This study examined data breaches in light of the user's routine activities. It did not consider external social or environmental factors. Additionally, the study used a single method: qualitative case study interviews. While we believe this method is most appropriate given our research questions, other methodologies may provide additional insight into these phenomena. A further limitation is that data gathered was self-reported and much of it retrospective. Self-report can provide valuable insight into an individual's experience of an event. However, information provided in this way cannot be assumed to be objectively accurate. Future use of objective measures that track individual behavior prior to and subsequent to a breach could be used to test the robustness of our findings.

Recruitment for this study employed self-selection and snowball sampling. We attempted to mitigate the potential biases of our sampling methods through purposive selection of those who entered our selection process. However, our final samples for both cases illustrate the tendency of snowball samples to reflect the characteristics of those recruiting. Further, our final sample was not representative of national demographics, a more diverse sample may have resulted in more transferable findings. While efforts were made to gather a representative sample of participants, restrictions of time, geography, and reach may limit the transferability of these findings.

Another limitation is the specific breaches selected: the Equifax and Facebook breaches were chosen because they affected a substantial portion of the US population and represented different types of data breach. However, it is possible that the selection of different breaches would result in different results. Additionally, during the process of data collection, it became evident that we would be unable to recruit an adequate number of Facebook participants in the available time frame. We thus expanded our inclusion criteria to allow users who were aware of the Facebook breach, but who were not notified that their data had been compromised. It is possible that using only participants whose data was breached would have yielded different results.

It is our hope that future research will mitigate these known limitations as well as any we have overlooked, and that this work will provide a foundation for future exploration into the relationship between users and those whose role it is to guard them from harm.

References

Adam, N. R., and Jones, D. H. (1989). Security of statistical databases with an output perturbation technique. Journal of management information systems, 6(1), 101-110.

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. European Journal of Information Systems, 26(6), 1-27.

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016a). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. European Journal of Information Systems, 25(4), 364-390.

Anderson, B. B., Vance, A., Kirwan, C. B., Jenkins, J. L., & Eargle, D. (2016b). From warning to wallpaper: Why the brain habituates to security warnings and what can be done about it. Journal of Management Information Systems, 33(3), 713-743.

Backhouse, J., and Dhillon, G. (1996). Structures of responsibility and security of information systems. European journal of information systems, 5(1), 2-9.

Baldwin, D. J., Buckley, J. P., & Slaugh, D. R. (2017). Insuring Against Privacy Claims Following A Data Breach. Penn St. Law. Review. 122, 683.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. Psychological review, 84(2), 191.

Bansal, G., and Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. Decision Support Systems, 71, 62-77.

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. European Journal of Information Systems, 1(2), 121-130

Beaudry, A. & Pinsonneault, A. (2010). The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use. MIS Quarterly, 34, 689-710.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. The journal of strategic Information Systems, 11(3), 245-270.

Bernard, H. R., Wutich, A., & Ryan, G. W. (2016). Analyzing qualitative data: Systematic approaches. SAGE publications.

Biernacki, P., & Waldorf, D. (1981). Snowball sampling: Problems and techniques of chain referral sampling. Sociological methods & research, 10(2), 141-163.

Bloomberg, L. D., & Volpe, M. (2018). Completing your qualitative dissertation: A road map from beginning to end. Sage Publications.

Bobko, P., Barelka, A., Hirshfield, L., & Lyons, J. (2014). Invited Article: The Construct of Suspicion and How It Can Benefit Theories and Models in Organizational Science. Journal of Business & Psychology, 29(3), 335–342.

Boockholdt, J. L. (1989). Implementing security and integrity in micro-mainframe networks. MIS Quarterly, 135-144.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly, 39(4), 837-864.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. International Journal of Cyber Criminology, 3(1), 400.

Burgoon, J., Buller, D., Ebesu, A., and Rockwell, P. (1994) Interpersonal deception: V. Accuracy in deception detection. Communication Monographs, 61(4), 303–325.

Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. 2009. Configuration of and interaction between information security technologies: The case of firewalls and intrusion detection systems. Information Systems Research, 20(2), 198-217.

Cavusoglu, H., Raghunathan, S., and Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. Journal of Management Information Systems, 25(2), 281-304.

Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. Mis Quarterly, 40(1).

Cohen, L. E., and Felson, M. (1979). “Social Change and Crime Rate Trends: A Routine Activity Approach,” American Sociological Review, 588-608.

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. MIS quarterly, 189-211.

Cremonini, M., & Nizovtsev, D. (2009). Risks and benefits of signaling information system characteristics to strategic attackers. Journal of Management Information Systems, 26(3), 241-274.

Creswell J. (2014) Research design: Qualitative, quantitative and mixed method approaches. London: Sage publications.

Crossler, R. E., & Posey, C. (2017). Robbing Peter to Pay Paul: Surrendering Privacy for Security’s Sake in an Identity Ecosystem. Journal of the Association for Information Systems, 18(7), 2.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. MIS Quarterly, 673-687.

DeMarrais, K. (2004). Qualitative interview studies: Learning through experience. Foundations for research: Methods of inquiry in education and the social sciences, 1(1), 51-68.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). The Sage handbook of qualitative research. Sage publications.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. Information Systems Journal, 19(4), 391-412.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 386.

Edmondson, A. C., & McManus, S. E. (2007). Methodological fit in management field research. Academy of management review, 32(4), 1246-1264.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. The Academy of Management Journal, 50(1), 25-32.

Goel, S., Williams, K., & Dincelli, E. (2017). Got Phished? Internet Security and Human Vulnerability. Journal of the Association for Information Systems, 18(1), 22.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation Network breach. MIS Quarterly, 41(3).

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Information systems journal, 24(1), 61-84.

Hodges, S. (2013). Examining the Gramm–Leach–Bliley Act's opt-out method for protecting consumer data privacy rights on the Internet. Information & Communications Technology Law, 22(1), 60-85.

Hua, J., & Bapna, S. (2013). The economic impact of cyber terrorism. The Journal of Strategic Information Systems, 22(2), 175-186

Jenkins, J. L., Anderson, B. B., Vance, A., Kirwan, C. B., & Eargle, D. (2016). More harm than good? How messages that interrupt can make us vulnerable. Information Systems Research, 27(4), 880-896.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. European Journal of Information Systems, 25(3), 231-251.

Kahneman, D. (2003). Maps of bounded rationality: Psychology for behavioral economics. American economic review, 93(5), 1449-1475.

Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. Mis Quarterly, 38(2).

Lee, C. H., Geng, X., & Raghunathan, S. (2016). Mandatory Standards and Organizational Information Security. Information Systems Research, 27(1), 70-86.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. MIS Quarterly, 71-90

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. Mis Quarterly, 173-186.

Lockman, A., & Minsky, N. (1984). Designing financial information systems for auditability. Journal of Management Information Systems, 1(1), 50-62.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. Information Systems Journal, 25(5), 433-463.

Luhmann, N. (1979). Trust and power. John Wiley & Sons.

Malhotra, N. K., Sung S. K., and Agarwal, J (2004), "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model", Information Systems Research, 15, 336-355.

Marshall, B., Cardon, P., Poddar, A., and Fontenot, R. (2013). Does sample size matter in qualitative research?: A review of qualitative interviews in IS research. Journal of Computer Information Systems, 54(1), 11-22.

Marshall, C., and Rossman, G. B. (2016). Designing qualitative research ed 6th. Sage publications.

Marston, C., Dixon, R., and Collier, P. (1989). Internal auditors and the prevention and detection of computer fraud. Journal of Information Technology, 4(4), 230

McKnight, D. H., Carter, M., Thatcher, J. B., and Clay, P. F. (2011). Trust in a specific technology: An investigation of its components and measures. ACM Transactions on Management Information Systems, 2(2), 12.

McKnight, D. H., & Chervany, N. L. (2000). What is trust? A conceptual analysis and an interdisciplinary model. AMCIS 2000 Proceedings, 382.

McKnight, D. H., and Chervany, N. L. (2001a). Trust and distrust definitions: One bite at a time. In Trust in Cyber-societies (pp. 27-54). Springer, Berlin, Heidelberg.

McKnight, D. H., and Chervany, N. L. (2001b). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. International journal of electronic commerce, 6(2), 35-59.

McKnight, D. H., Choudhury, V., and Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information systems research, (13:3), 334-359.

Miles, M. B., Huberman, A. M., and Saldaña. J. (2014). Qualitative Data Analysis: A Methods Sourcebook (3nd ed.). Thousand Oaks, CA: Sage.

Mumford, E. (1998). Problems, knowledge, solutions: solving complex problems. The Journal of Strategic Information Systems, 7(4), 255-269.

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: making sense of information technology in organizations. ACM Transactions on Information Systems, 12(2), 174-207.

Phillips, D. J. (1998). The social construction of a secure, anonymous electronic payment system: frame alignment and mobilization around Ecash. Journal of Information Technology, 13(4), 273.

Png, I. P., Wang, C. Y., & Wang, Q. H. (2008). The deterrent and displacement effects of information security enforcement: International evidence. Journal of Management Information Systems, 25(2), 125-144.

Png, I. P., & Wang, Q. H. (2009). Information security: Facilitating user precautions vis-à-vis enforcement against attackers. Journal of Management Information Systems, 26(2), 97-121.

Ponemon Institute (2017a) 2017 Cost of Cyber Crime study.

Ponemon Institute. (2017b). 2017 Cost of Data Breach Study: Global Overview.

Pratt, M. G. (2009). From the editors: For the lack of a boilerplate: Tips on writing up (and reviewing) qualitative research. Academy of Management Journal, 52(5), 856-862.

QSR International. (2019) “What is NVivo?” Retrieved from : https://www.qsrinternational.com/nvivo/what-is-nvivo

Rainer Jr, R. K., Snyder, C. A., & Carr, H. H. (1991). Risk analysis for information technology. Journal of Management Information Systems, 8(1), 129-147.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. Information Systems Research, 20(1), 121-139.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. Criminal justice and behavior, 38(11), 1149-1169.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816-826.

Rhee, H. S., Ryu, Y., & Kim, C. T. (2005). I am fine but you are not: Optimistic bias and illusion of control on information security. ICIS 2005 Proceedings, 32.

Ridder, H. G. (2017). The theory contribution of case study research designs. Business Research, 10(2), 281-305.

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. Qualitative research in psychology, 11(1), 25-41.

Romanosky, S., & Acquisti, A. (2009). Privacy costs and personal data protection: Economic and legal perspectives. Berkeley Tech. Law Journal, 24, 1061.

Rountree, P. W., & Land, K. C. (1996). Burglary victimization, perceptions of crime risk, and routine activities: A multilevel analysis across Seattle neighborhoods and census tracts. Journal of research in crime and delinquency, 33(2), 147-180.

Rubin, H. J., & Rubin, I. S. (2011). Qualitative interviewing: The art of hearing data. Sage.

Schneier, B. (2009). Schneier on security. John Wiley & Sons.

Saldaña, J. (2016). The coding manual for qualitative researchers. Sage.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. Journal of Management Information Systems, 32(2), 314-341

Shankar, V., Urban, G. L., & Sultan, F. (2002). Online trust: a stakeholder perspective, concepts, implications, and future directions. The Journal of strategic information systems, 11(3), 325-344.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security" De Jure" Standard in a Government Organization. MIS Quarterly, 463-486.

Solon, O. 2018. “Facebook says Cambridge Analytica may have gained 37m more users' data” The Guardian: US edition, April 4 2018. Retrieved from: https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought

Straub Jr, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: a field study. MIS quarterly, 45-60.

Straub Jr., D. W. & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. Management Information Systems Quarterly, 22(4), 441.

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. Journal of Management Information Systems, 22(4), 109-142.

Tow, W. N. F. H., Dell, P., & Venable, J. (2010). Understanding information disclosure behaviour in Australian Facebook users. Journal of Information Technology, 25(2), 126-136.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). Journal of the Association for Information Systems, 15(10), 679.

VanWynsberghe, R., & Khan, S. (2007). Redefining Case Study. International Journal of Qualitative Methods, 80–94.

Vizetelly, F. H. (1936). The Modern Home and Office Dictionary. Funk and Wagnalls Company. New York and London.

Vuorinen, J., & Tetri, P. (2012). The Order Machine-The Ontology of Information Security. Journal of the Association for Information Systems, 13(9), 695.

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. MIS Quarterly, 39(1).

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: an investigation of antecedents and consequences. Information Systems Research, 28(2), 378-396.

Warkentin, M., Johnston, A. C., Walden, E., & Straub, D. W. (2016). Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. Journal of the Association for Information Systems, 17(3), 194.

Williams, M. L. (2015). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. European Journal of Information Systems, 15(4), 403-414.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research Note—Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. Information systems research, 25(2), 385-400.

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. Journal of Management Information Systems, 27(1), 273-303.

Yar, M. 2005. The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, (2:4), pp. 407-427.

Yin, R. K. 2003. *Case Study Research and Applications: Design and Methods 3rd ed.* Sage publications

Yin, R. K. 2018. *Case Study Research and Applications: Design and Methods 6th ed.* Sage publications

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. Journal of the Association for Information Systems, 16(6), 448.

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing interdependent information security risks: Cyberinsurance, managed security services, and risk pooling arrangements. Journal of Management Information Systems, 30(1), 123-152

Appendix A

Recruitment Flyer

University of Memphis

Participants Wanted for a Research Study

Examining Breach and Post-Breach Behaviors and Attitudes

The goal of this study is to increase our understanding of the behaviors and assumptions individuals make related to their data and how it is protected and the effects that being the victim of a data breach has on those behaviors and assumptions. If you choose to participate, you will be asked a series of questions about your attitude, behaviors, and experiences. This will take approximately one hour.

By doing this study, we hope to learn about how data breaches affect people.

You must be at least 18 years old to participate. You must be a US resident to participate. To participate, you must have been a victim of either the Equifax data breach, the Facebook data breach, or both.

To learn more about this research, contact Ruby Booth (rbooth@memphis.edu).

This research is conducted under the direction of Dr. Sandra Richardson, Associate Professor of Business Information and Technology at the University of

Memphis. To contact Dr. Richardson email
srchrdsn@memphis.edu

Recruitment Social Media post

University of Memphis

Participants Wanted for a Research Study
please share

Examining Breach and Post-Breach Behaviors and Attitudes

The goal of this study is to increase our understanding of the behaviors and assumptions individuals make related to their data and how it is protected and the effects that being the victim of a data breach has on those behaviors and assumptions. If you choose to participate, you will be asked a series of questions about your attitude, behaviors, and experiences. This will take approximately one hour.

By doing this study, we hope to learn about how data breaches affect people.

You must be at least 18 years old to participate.
You must be a US resident to participate. To participate, you must have been a victim of either the Equifax data breach, the Facebook data breach, or both.

To learn more about this research, contact Ruby Booth (rbooth@memphis.edu).

This research is conducted under the direction of Dr. Sandra Richardson, Associate Professor of Business Information and Technology at the University of Memphis. To contact Dr. Richardson email srchrdsn@memphis.edu
please share

Recruitment Email

Subject Line: Participants being sought for a voluntary data breach research study

This email message is an approved request for participation in research that has been approved or declared exempt by the University of Memphis Institutional Review Board (IRB).

You are being invited to take part in a research study about data breaches. If you volunteer to take part in this study, you will be one of approximately 50 people to do so.

The goal of this study is to increase our understanding of the behaviors and assumptions individuals make related to their data and how it is protected and the effects that being the victim of a data breach has on those behaviors and assumptions. If you choose to participate, you will be asked a series of questions about your attitude, behaviors, and experiences. This will take approximately one hour.

You must be at least 18 years old to participate.

You must be a US resident to participate.

To participate, you must have been a victim of either the Equifax data breach, the Facebook data breach, or both.

By doing this study, we hope to learn about how data breaches affect people.

This research is conducted under the direction of Dr. Sandra Richardson, Associate Professor of Business Information and Technology at the University of Memphis. To contact Dr. Richardson email srchrdsn@memphis.edu

To learn more about this research, contact Ruby Booth (rbooth@memphis.edu).

Feel free to forward this message to anyone you think might be interested in participating!

Thank you.

Appendix B

Consent for Research Participation

Title	Examining Breach Behaviors: Individual Change in the Aftermath of Information Compromise
Researcher(s)	Ruby Booth, University of Memphis Sandra Richardson, University of Memphis
Researchers Contact Information	901-484-8685, rbooth@memphis.edu srchrdsn@memphis.edu

You are being asked to participate in a research study. The box below highlights key information for you to consider when deciding if you want to participate. More detailed information is provided below the box. Please ask the researcher(s) any questions about the study before you make your decision. If you volunteer, you will be one of 30-80 people to do so.

Key Information for You to Consider

Voluntary Consent: You are being asked to volunteer for a research study. It is up to you whether you choose to participate or not. There will be no penalty of loss of benefit to which you are otherwise entitled if you choose not to participate or discontinue participation.

Purpose: The goal of this study is to increase our understanding of the behaviors and assumptions individuals make related to their data and how it is protected and the effects that being the victim of a data breach has on those behaviors and assumptions. If you choose to participate, you will be asked a series of questions about your attitude, behaviors, and experiences.

Duration: This will take approximately 60 minutes and addition 30 mins follow up may occur to clarify responses.

Procedures and Activities: You will be asked to answer questions about your perceptions about how your data is/was protected, your online routines, and your reactions to discovering that you were affected by a data breach. You will need to be interviewed by a researcher once during this subject and may be contacted to clarify or elaborate on your answers in a follow up phone call in the weeks after your interview. Interviews may take place on campus at University of Memphis or by phone. You will be asked if you permit audio recording of the interview.

Risk: To the best of our knowledge, the things you will be doing have no more risk of harm than you would experience in everyday life.

Benefits: You will not get any personal benefit from taking part in this study. Your willingness to take part, however, may, in the future, help society as a whole better

understand this research topic.
Alternatives: Participation is voluntary, and the only alternative is to not participate.

Who is conducting this research?
Ruby Booth, LI of the University of Memphis, Department of Business Information and Technology is in charge of the study. Her faculty advisor is Sandra Richardson. There may be other research team members assisting during the study.

Why is this research being done?
The purpose is to increase our understanding of the behaviors and assumptions individuals make related to their data and how it is protected and the effects that being the victim of a data breach has on those behaviors and assumptions. You are being invited to participate because you were affected by the Equifax or Facebook data breaches. You are 18 years of age or over, not currently incarcerated, and are not now nor have ever been an employee of the company associated with your data breach.

How long will I be in this research?
The research will be conducted at University of Memphis. The interview should take about one hour. After the interview you will receive a transcript of your comments, to which you may make corrections or clarifications. Correcting or clarifying your statements, if necessary, may take approximately 30 mins. The total amount of time you will be asked to volunteer for this study is approximately one hour on the day of your interview and approximately 30 mins for clarification in the weeks following your interview.

What happens if I agree to participate in this Research?
If you agree you will be asked to answer questions about your online routines, your beliefs about organizations that protect your data, and how data breach affects those beliefs and actions. These questions will take the form of an interview, which will either take place on the University of Memphis campus or by phone. With your consent, the audio of interview will be recorded to ensure accurate transcription of your responses. You may also be contacted in the weeks following your interview to clarify comments you have made. Throughout this process you can skip any question that makes you uncomfortable or that you do not wish to answer for any reason. You can, also, stop any time. We will tell you about any new information that may affect your willingness to continue participating in the research. We will also provide you with a copy of the final report, if you wish.

What happens to the information collected for this research?
Information and recordings collected for this research will be used to create a model of people’s decision making about what they do online before and after experiencing a data breach. We may publish and/or present the results of this research. However, your information will be combined with information from other people taking part in the study. When we write about the study to share it with other researchers, we will write about the

combined information we have gathered. We may publish the results of this study; however, you will not be personally identified in these written materials.
After the completion of this research all recordings will be deleted. Transcripts and related documents will be purged of identifiable data and stored for no longer than five years under lock and/or on secure computers. After five years all data will be destroyed. Paper materials will be shredded. Digital materials will be deleted.

How will my privacy and data confidentiality be protected?
We promise to protect your privacy and security of your personal information as best we can. Although you need to know about some limits to this promise. Measure we will take include:
All information gathered -- including notes, interview transcripts, and consent documents -- will be kept in a locked environment or on password protected computers. We will make every effort to prevent anyone who is not on the research team from knowing that you gave us information, or what that information is.
After the completion of this research all recordings will be deleted. Transcripts and related documents will be purged of identifiable data and stored for no longer than five years under lock and/or on secure computers. After five years all data will be destroyed. Paper materials will be shredded. Digital materials will be deleted.
We will keep private all research records that identify you to the extent allowed by law. However, there are some circumstances in which we may have to show your information to other people. Individuals and organization that monitor this research may be permitted access to inspect the research records. This monitoring may include access to your private information and audio recordings. These individual and organization include:
Institutional Review Board
Law Enforcement officials in the event of a disclosure required by law.

What if I want to stop participating in this research?
It is up to you to decide whether you want to volunteer for this study. It is also ok to decide to end your participation at any time. There is not penalty or loss of benefits to which you are otherwise entitled if you decided to withdraw your participation. Your decision about participating will not affect your relationship with the researcher(s) or the University of Memphis.

As described above, you will be audio recorded while performing the activities described above. Audio recording will be used for creating a transcript of your answers to study questions. Initial the space below if you consent to the use of audio recording as described

____ I agree to the use of audio recording.

With your permission, your name will be used in follow up emails to you asking for clarifications of your comments. Initial the space below if you consent to the use of your name as described

___ I agree to the use of my name in study correspondence.

Name of Adult Participant	**Signature of Adult Participant**	**Date**

Researcher Signature (To be completed at the time of Informed Consent)

I have explained the research to the participant and answered all of his/her questions. I believe that they understand the information described in this consent form and freely consent to participate**.**

Name of Research Team Member	**Signature of Research Team Member**	**Date**

Appendix C

Eligibility Questions Survey

Thank you for agreeing to participate in this study. I'd like you to remind you that if there are questions you do not want to answer or if you wish to stop at any time, you are free to do so with no consequences.
What is your age?

○ 18+, include
○ Below 18, exclude

Were you notified that your data had been compromised by the Equifax data breach?

○ Yes, include
○ No, exclude from Equifax questions

Were you notified that your data had been compromised by the Facebook data breach?

○ Yes, include
○ No, exclude from Facebook questions *(revised to allow inclusion for awareness)*

Have you ever been an employee of Equifax?

○ Yes, exclude from Equifax questions
○ No, include

Have you ever been an employee of Facebook?

○ Yes, exclude from Facebook questions
○ No, include

What is your gender?

○ Male
○ Female
○ Non-binary

What is your ethnicity?

○ Caucasian / White
○ African American / Black
○ Hispanic / Latino or Latina
○ American Indian or Alaskan Native
○ Asian
○ Native Hawaiian or Other Pacific Islander
○ Mixed Race
○ Other ____________________

What is your age?

○ Under 18
○ 18-24 years old
○ 25-34 years old
○ 35-44 years old
○ 45-54 years old
○ 55-64 years old
○ 65-74 years old
○ 75 years or older

What is your highest level of education?

○ High School
○ Some College
○ Associates Degree or Professional Certification
○ Bachelor's Degree
○ Some Graduate School
○ Graduate Degree or Professional Degree

What is your approximate household income?

○ Less than $25,000.
○ $25,000 to $34,999.
○ $35,000 to $49,999.
○ $50,000 to $74,999.
○ $75,000 to $99,999.
○ $100,000 to $149,999.
○ $150,000 to $199,999.
○ $200,000 or more.

Appendix D

Interview Script

Introduction

“Thanks for taking the time to talk with me. I’m doing research to investigate people’s online routines. I’m particularly interested in how you view those responsible for protecting your data and how your behaviors may have changed after you were notified that your data was affected by a breach.”

May I record this interview?

May I take notes of our conversation?

We also usually send copies of your transcript to allow you to check for accuracy. Would you like that?

Thank you for agreeing to participate in this study. Remember, we can stop at any time, and any questions that you do not feel comfortable answering we can skip.

I’d like to start with your current behaviors online.

[Note: The terms in brackets indicate the text used for each breach. Participants who experienced the Equifax breach are asked about financial activities and attitudes towards Equifax. Participants who experienced the Facebook breach are asked about social activities and attitudes towards Facebook.]

I.
   a. I’m interested in your routines online. What kinds of routine [financial / social] activities do you usually do online in a typical day?
   b. Tell me about any safety precautions you routinely take online to protect yourself or your [financial / social] data.

II. You were notified that your data had been compromised in the [Equifax/Facebook] breach.

a. How were you notified about the security breach that affected your data?
b. How did the notification affect your view of how risky you think it is to give your data to [financial/ social media] companies that operate online?
c. Did that feeling of risk affect your perception of [Equifax/Facebook]'s ability to provide protection for your data?
d. How did the notification affect your confidence in your own ability to protect your information and information systems online?
e. How does that confidence in your own ability to protect your information and information systems online affect your beliefs about [Equifax/Facebook]'s ability to provide protection for your data?
f. How did the notification affect your sense of trust that [Equifax/Facebook] would be willing and able to protect your data?
g. Some people are more innately suspicious than others. Are you more suspicious (inclined to believe that people are generally out for their own best interests) or lacking suspicion (inclined to believe that they generally have other's best interests at heart), since the breach?
h. How do your feelings of suspicion affect your perception of [Equifax/Facebook]'s ability to provide protection for your data?
i. Did you take specific steps [like signing up for LifeLock or freezing your credit / Leaving Facebook, changing your privacy settings, or giving up use of third-party apps on Facebook]?

i. [if they use LifeLock due to a free subscription] Will you continue to subscribe to LifeLock after your free year expires?

j. How well do you think [Equifax/Facebook] is protecting your data now?

k. Do you think [Equifax/Facebook] is doing anything differently now to keep your data secure?

III.

a. How are your routine [financial / social] activities online different, since you were notified of the breach?

b.] What specific changes did you make to your online routines after you were notified of the breach?

c. How does your current perception of [Equifax/Facebook]'s ability to protect your data affect your online activities?

d. Did you start taking any particular routine safety online precautions after you were notified of the breach?

e. How does your current perception of [Equifax/Facebook]'s ability to protect your data affect the safety precautions that you take routinely since you were notified about the breach?

f. Can you think of anything else that changed about what you routinely do online or how you do it as a result of being notified about the breach?

IV. I'd like you to think back, if you can, to *before* you received notification of the breach.

a. What was your perception of [Equifax/Facebook]'s ability to provide protection for your data before the breach?

b. did you know about [Equifax/Facebook]'s data collection before the breach?

c. How did the breach change your perception of [Equifax/Facebook]'s ability to provide protection for your data?

V. We are looking at whether breach notifications change an affected person's beliefs, characteristics, or behaviors. The questions I'm about to ask are about the way you felt and acted before you were notified that your data had been affected by the breach.

a. I'm interested in how your online routine was changed by being notified about the breach. What kinds of [financial / social] activities did you usually do online in a typical day, before being notified about the breach?

b. How did your perception of [Equifax/Facebook]'s ability to protect your data affect those activities?

c. Tell me about any safety precautions you routinely took online to protect yourself or your [financial/ social] data before being notified about the breach.

d. How did your perception of [Equifax/Facebook]'s ability to protect your data affect the safety precautions you took before being notified about the breach?

VI. One of the things we are trying to understand is how changes to a person's individual characteristics such as attitudes and abilities affect the way you perceive those who are responsible for protecting your data.

a. Prior to being notified about the breach, how risky did you think it was to give your data to [financial/ social media] companies that operate online?

b. How did those perceptions of risk affect your perception of [Equifax/Facebook]'s ability to protect your data?

c. Prior to being notified about the breach, how confident did you feel about your own ability to protect your information and information systems online?

d. Prior to being notified about the breach, how did your level of confidence in your own ability to protect your information and information systems online affect your perception of [Equifax/Facebook]'s ability to provide protection for your data?

e. We trust companies to act in certain ways in certain situations. Prior to being notified about the breach, to what extent did you trust that [Equifax/Facebook] would be willing and able to protect your data?

f.

   i. Prior to being notified about the breach, were you inclined to believe that people are generally out for their own best interests or that they generally have other's best interests at heart?

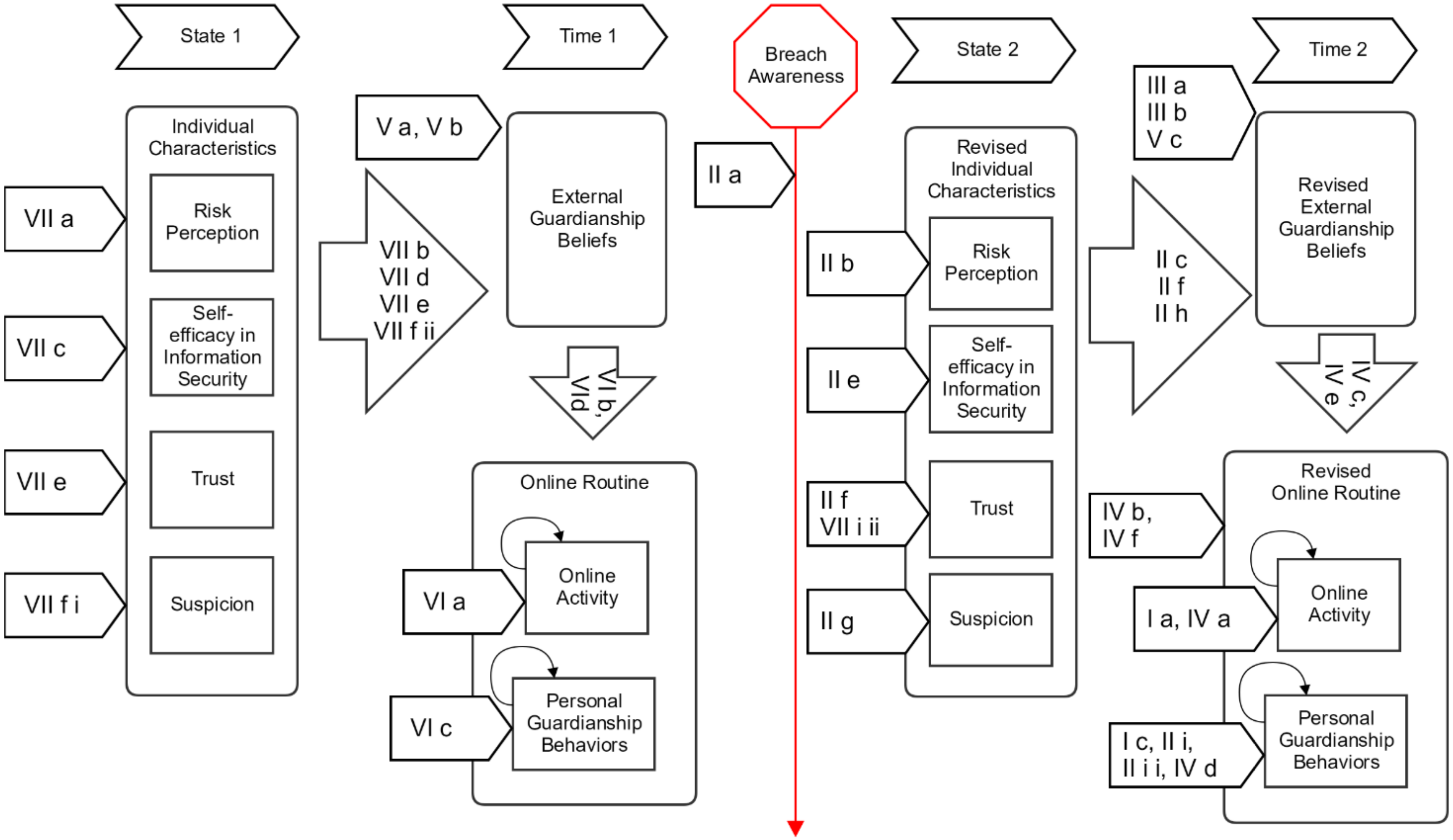
   ii. Prior to being notified about the breach, how did your suspicion affect your perception of [Equifax/Facebook]'s ability to protect your data?

VII. Is there anything further you would like to share with me about your experiences?

VIII. Would you like a copy of our final research document when it is complete?

Appendix E

Questions Mapped to Research Model



Appendix F

Equifax: Stage One Codes

Primary Code	Sub-code	Sub-code’s sub-code
Attacker skill level		--
Breach	Breach Awareness Breach Notification Number of breaches	--
Business model	--	--
Comparison	--	--
Competition	--	--
Complacency	--	--
Consequences	--	--
Convenience	--	--
Corporate Nature	--	--
Data Characteristics	Amount of data Data value Sensitive data	--
Data collection	--	--
“Do not know”	--	--
“don't know what else to do”	--	--
Duty of care	--	--
Ease of Use	--	--
“embarrassing for them”	--	--
External Guardianship Beliefs	--	--
“extra safety precautions”	--	--
Fear	--	--
Higher standard	--	--
Human nature	--	--
“I did not think about Equifax”	--	--
“I don’t feel like Equifax is part of my community”	--	--
“I do not think very often about who is protecting my data”	--	--
“I would hope”	--	--
Individual Characteristics	Risk Perception, Self-Efficacy in Information Security, Suspicion, Trust	--
“keep an eye on it”	--	--
Lack of Awareness	--	--
Lack of Care	--	--
Likelihood of being targeted	--	--

Primary Code	Sub-code	Sub-code's sub-code
Mandatoriness	--	--
Mistakes	--	--
"my reputation"	--	--
No control	--	--
No effect	--	--
Not a customer	--	--
"on their own side"	--	--
Past experience of fraud	--	--
Poverty vs Wealth	--	--
Regulation	--	--
Responsibility on user	--	--
Risk Minimization	--	--
Safety measures	--	--
Security expertise	--	--
Selling data	--	--
"shocked but not surprised"	--	--
"skeptical"	--	--
Superficial change	--	--
"the dark web"	--	--
"the product"	--	--
Third party	--	--
Tiering data	--	--
"trigger moment"	--	--
Unintentional change	--	--
User Online Routine	Online Activity	--
	Personal Guardianship Behaviors	Information Restriction, Layered security, Obstacles, Passwords
Where I work	--	--

Appendix G

Participant Narratives

P001

P001 was affected by the Equifax breach. She is a white woman, between 35-44 years of age. She holds a bachelor's degree in the Humanities, has worked primarily in the service industry, and reports a household income between $35,000-$49,000. Her face-to-face interview took place on Feb 26, 2019.

Prior to the Equifax breach P001 says "I did not think about Equifax at all." She reports, "I knew that people were collecting my data. I knew that there were data collectors out there in the world. I did not know really about Equifax specifically, until the breach." P001's online financial routines at that time were similar to her routines today. However, in the past two years, her financial situation improved substantially. Thus, she reports some changes due to her improved financial stability. In 2016 and late 2017, she was not as willing to check financial information such as her credit score, both due to mistaken beliefs "I was under the impression that checking my credit score too often would hurt my credit score" and anxiety about her financial standing "Also, I was afraid of what I would see." Today she checks her credit score regularly, not as a personal guardianship behavior resulting from the breach, but because "[showing her credit score] is something that [her] credit card actually does for me which is pretty sweet."

Prior to the breach, P001's personal guardianship behaviors were limited to a set of common passwords that she uses on various sites. Fear of forgetting passwords motivates this repetition of use: "If they make me come up with a unique password, I end up having to do the 'I've forgotten my password' thing every single time I log in." In addition to the use of passwords, she tried not to access financial information on unsecured networks. “Like, I wasn’t gonna go to the library and access my bank information. I was going to do that from trusted machines. I, I don’t think I used the school computers for any kind of financial information.” Today, her guardianship behaviors are much the same, though she reported that she now tries to only access financial information “at home and on [her] own WiFi.” She is also more “attentive to spam emails,” because she is concerned “about people emailing me viruses by accident.”

Prior to the breach, P001 perceived there being a “a small amount of risk” in giving data to financial organizations that operated online. She felt that her own risk was small, because she had little financial stability. “It seemed to me like something that only people with financial stability need worry about, because I had so little to lose” She still feels this way. Though she reports “actively trying to change that right now, because … being financially stable, I feel like I should protect that stability more.”

P001 both now and in the past reports very low feelings of self-efficacy in information security. In the past, “I did not feel confident. I knew that I was doing my best.” And today,” I do not think of myself as protecting my information very well. And so, it really didn’t change my self-assessment of my ability to protect my information. I just kind of count on my information being lost in the shuffle.”

When it comes to trust in Equifax or in companies in general, P001 reports that she is “inherently a bit skeptical.” She was reluctant to attribute protective qualities to Equifax, due to their collection and use of individuals’ data without their consent. “I think there’s sort of a definition of protection. Like, they weren’t asking us what we wanted them to do with [our data].” Prior to the breach, she did believe that large companies like Equifax would “protect [data] from hackers.” After the breach, her immediate thought was, “oh, well, people are collecting our data, and they’re not taking care of it *at all*.”

P001 reports a fairly high faith in humanity. This extends to individuals working for Equifax, who she sees as “as basically just normal people who have standard level of flaws and abilities.” This view seems to affect her tolerance of breaches: “people make mistakes in every profession, and when people make mistakes in financial professions it affects people’s financial, ah, standing.” Her low SEIS also affects her view of these individuals within the organization charged with guardianship: “Honestly, I think they are probably better at it than I am. But that’s not saying very much, because I’m not very good at protecting by data.”

Overall P001 rarely, if ever, thought about Equifax as a data guardian prior to the data breach. After the data breach, once the firm came to her attention, she views them as she does all companies that hold her data. “For the most part, if a company has my data, I trust it to look after my data if it is in their best interests to look after my data.” When it comes to Equifax, she feels that they are probably doing more to protect her data than they were, because the breach was “hugely embarrassing for them.” “I think they probably implemented new safety protocols. And I think probably what led to the breach was, just, given a certain amount of time and uniformity of behaviors, people get a little lackadaisical about things. They stop worrying about things, because there hasn’t been a problem. And so when there is a problem they’re like: Oh! And they tighten everything up.” She does not view Equifax negatively for the breach itself, which she sees as an inevitable part of the environment now. “I just sort of picture [data breaches] as like car accidents. They happen sometimes. They don’t happen sometimes. I don’t feel like I have a lot of control over the situation.”

P001’s primary concern about data breaches is not financial. She worries instead about the compromise of her social media accounts. “I feel like people respect me and my opinion on certain matters, that there are areas where I have expertise and areas in which I’ve built trust in my peers and my community that I really value, and the thought of someone hacking into my social media scares me more, because it could ruin my reputation.”

P002

P002 was affected by the Equifax breach. He is a white man, between 35-44, who holds a bachelor's degree. He works in the Healthcare field and reports an annual household income of $100,000-149,000. His face-to-face interview took place on March 2, 2019. P002 is one of the participants for whom the Equifax breach was a trigger moment. "It was sort of like a trigger moment.… It was more like, well, I guess it's getting worse, so let's do something." Prior to the breach his online financial routines consisted of checking his banking account daily, his credit cards monthly, and his stock portfolio when there were market fluctuations. These have not changed meaningfully since the breach. What has changed are his personal guardianship behaviors. Both before and after the breach he implements two-factor identification whenever possible. However, prior to the breach he used "pretty much the same [passwords] across the board." Now he has changed to password phrases. However, he still describes his passwords as "terrible and not very secure."

When it comes to selecting protective measures, P002 uses a tiered system with passwords chose by risk level. For what he considers low risk sites such as this mortgage company, he uses simpler passwords. He considers credit card company sites to be medium risk. High risk site, such as his bank account, are given the highest amount of security including fingerprint-based log-on access and complex passphrases.

P002 "basically assumed that [financial companies] were insecure," even prior to the Equifax breach. But he expressed surprise that "Equifax would be the first that I would hear from." He explained that this surprise came from a belief prior to the breach that given the amount and sensitivity of the data Equifax held, that they would keep their data "locked down." He knew about Equifax and their data collection, but did not think of them except when accessing his credit report. His perception of their ability as guardians did not affect his behavior on other sites.

In terms of his own ability to protect his data, P002 feels that he is above average, but draws a clear distinction between the protections an above average user is capable of that that of a security expert. "I am not a security expert. Nor do I have one on my staff." "I assumed they would be better."

After the breach, P002 examined his beliefs about Equifax and came to the following conclusion. "What that makes me think of is, you know, is Equifax more inclined to hire people or to have in place better rules. I don't think it has anything to do with me. I mean, now that I think about it, there's no real incentive, because I'm not paying them anything. So why should they protect my data? If their actual clients, if their data was breached then I think they have I think they have more incentive to protect that. And if there were more competition, they would be more interested in holding onto my data. But there's not lot of competition. It's not like if my data gets out there...it's not like a credit card company is going to check with the hackers to get it. So it doesn't change anything for Equifax to have my data available to somebody else. Like my data has no real value except that they have it. Like, either they have it or they don't. If someone else has it Equifax doesn't really lose anything by getting hacked. It's not like the data is gone. So I guess my suspicion is kind of warranted really. There's no incentive for them. "

P002 sees the changes that Equifax made as cosmetic: "they did a PR thing." He doubts their willingness to provide additional guardianship, because "they have no more incentive now other than the bad PR." He argues, "their business model is still the same."

His overall sentiment towards Equifax is quite negative: “So I'm the product they don't care so much about, right? So, yeah, I'm very suspicious of that. And why would I trust that, right?” He sees the company as “beholden to their shareholders….that's not me, right? Unless I'm a majority shareholder in the company.” His view of individual differs however, even when discussing individuals working for Equifax: “people are different. You know, if I talked to a person, they might be more interested in my wellbeing.”

When asked if there was any addition information he would like to share, P002 told the story of why he stopped using the Facebook app:

“I stopped using Facebook a couple of years ago, because they were doing some weird experimental things on Android users….I read an article that Facebook was doing a social experiment to see how many crashes it would take for someone to uninstall the app. And when my app started crashing, frequently, more frequently it had been, I assumed I was part of that program. … I uninstalled it because I assumed that was part of the program, not because it was actually crashing. Because that made me feel much more suspicion that they were actively doing things. Made me much more suspicious. And then, I mean, you go off and on Facebook because you kind of have to sometimes it feels like, from a social perspective, but, um but I've never installed the app again.”

P003

P003 was affected by the Facebook breach. She is a white woman, between the ages of 35 -44, who holds a graduate or professional degree. Her approximate annual household income is $150,000 - 199,999. Her phone interview took place March 4, 2019.

P003's primary online social media activities are Facebook, Nextdoor, and YouTube. On the latter two platforms, she describes herself as "more of a consumer, than a producer." Though she does occasionally "upload home videos of the dog and baby" to YouTube. Her online activity in terms of where she goes online didn't change much due to the breach. Her son was born after the breach, though, so her posting frequency on YouTube did increase due to that life change.

P003's safety precautions include limiting the information she puts online: "I try to only give information that I absolutely have to, like as far as stuff on my profile." She is also quite conscious of who can view the content she does post. Some content she sees as acceptable for public view "so the dog, like, okay, so most all of my videos are public." Other content she creates for her close social network. "[Videos] that have my son in it. Those are unlisted. Because I want to be able to share the links with like my parents, my in-laws, my family. But I don't want anyone else to really see the video."

Prior to the Facebook breach, P003 felt that using Facebook and other social media was fairly low risk. She thought the risk was "pretty directly proportional to your security, to your behavior. Like I thought the risk to my privacy was, like, what are my privacy settings, what is my password, do I share password." Now she feels much less secure, because she no longer sees her own actions as defining her security. "So that was kind of--- kind of eye opening to me like in some sense it doesn't matter how careful I am. You know, the issue was with my friend. If I have a friend who isn't then my data is out there…. And I have obviously not control or no visibility into what my friends are doing so it's not like you know I can go to my friends like and be like this one's not going to be responsible"

P003 was then and is now fairly suspicious of companies in general but felt that Facebook was "Like on a scale of 0-10 where 0 is like you know wholly unethical and 10 is perfectly ethical, I thought that they were like an eight. You know. Pretty good." Now she views them fairly negatively: "Oh, God, like, 3, 4?" Even so, she says, "I mean I didn't have that moment of: I trusted Facebook and the violated my trust." She says, "I guess I never had a whole lot of faith in Facebook to protect my data. So, in that sense, I guess in some ways I was kind of surprised that it happened and in others I wasn't."

P003 even questions Facebook's true business model at this point. "Like maybe they are just kind of in…like maybe their business isn't entirely social media, maybe their business is collecting data and selling it." She doesn't believe that Facebook has improved its security, but instead thinks that "to be honest I think maybe they are just trying to not get caught, as of now."

The Facebook breach made P003 much more cautious of what she puts on social media. "Um, it definitely made me more mindful about just not giving away more data than I need to on anything. If I'm setting up a profile for anything, for grubhub, whatever, I just don't give any more information than I absolutely have to." The breach also affected how she feel about using social media. "I guess just inwardly I just accepted that my data is being used in ways that I did not consent to. Maybe that's just the price of using Facebook."

P003 feels in some ways trapped by Facebook:

So if it were not for my family being so active on Facebook, I would not do it. But it’s an easy way to connect with my parents, my siblings, and my friends too. But I would sacrifice that for my friends, but I won’t for my family. Like, so, my husband quit Facebook after that happened. And he said he just doesn’t want Facebook to have his data, that he doesn’t think Facebook deserves to have him as a consumer of their product. And I kind of feel the same way. Like they don’t really deserve it. Like I’m not using Facebook because I support them. I’m just using it because I want to keep in touch with my family and it’s the easiest way.

And in that way it kind of feels bad. It kind of feels like emotional blackmail kind of thing. Like, we’re not going to protect your data but if you don’t use us then your kind of cut off from your family, because they all use Facebook and they’re not going to quit.

By far the most emotionally charged and barbed issue for P003 concerns her young son:

Um, so I’ve just kind of accepted that my data is going to be out there. But that’s kind of weird. You know, like, I find I feel exposed in a way that I didn’t expect to. I have put pictures of my son on Facebook. So I’m sure his face is in some facial recognition software out there. I don’t know exactly how I feel about it. Whether I should just…I should have been, like really strict, like not putting any pictures of him on Facebook. My family will just have to deal with it. We can text and do other sorts of things. Or if like it’s unavoidable, like, even if I don’t put pictures of him on Facebook like someone else might. Like an aunt or whatever. And what am I going to do, like, tell them not to? Right, so I think I have just kind of accepted that um data breaches happen and are happening probably. And I don’t know how I feel about that yet. Especially will my son.

Because I can make a choice to have a Facebook profile and to put whatever I want up there. But I’m posting his pictures on Facebook without his consent. Yeah, so I don’t know how I feel about that yet. I feel weird about it, but it’s going to take some time for me to process.

P004

P004 was affected by the Equifax data breach. He is a white male, between 35-44, who holds a bachelor's degree. He reports an approximate annual household income of $200,000 or above. His

P004 describes himself as "a data person." He finds looking online at records of purchases made or things he's done enjoyable. As a result, he reports reviewing purchases and investments fairly often both before and after the breach. P004 does not see a relationship between his online activity (where he goes and what he does) and his view of Equifax as a data guardian, either before or after the breach.

Prior to the data breach he did not think much about Equifax. Despite knowing that Equifax had "an enormous amount of data," he didn't spend "any time thinking about, like, what kind of security they might have in place, or even thinking about the fact that they would be a relatively detrimental target if someone did target them." Once he was notified of the breach he "went from not having a perception necessarily to having a perception that they suck." Negative phrasing is present throughout his interview in which he described Equifax variously as "morons" and "the evil you can't do without." He feels that any changes Equifax made to their security is "just superficial."

Prior to the breach, P004 believed, in general, that "a company the size of Equifax would have been more successful at taking the long-term view and realizing what they need to do to be successful over a longer period of time." He felt that organizations were generally better as assessing their best interests than individuals and that firms' best interests over time generally align with pro-social action. In his own words, "I do believe that companies that have a long view on what is best for them generally will do things that are best for everybody…. But the companies that are more short-sighted about that can act to the detriment of society." After the breach, he revised this view: "I think that the Equifax data breach highlighted fact that companies can be just a stupid as individuals."

In terms of his own behaviors, he uses strong passwords and a password manager online. He also now uses different passwords for every site. He is unsure whether this can be attributed the Equifax breach, rather than to improvements in password management technology. As a result of the breach, he did consider freezing his credit, but decided that ongoing job searches made this step too inconvenient.

P004 does not see himself as particularly able to protect himself online, despite a fair amount of technical knowledge. He believed before the breach that "if [he] used the tools that were available then [he] would be more secure." But he views himself as dependent upon the companies to be able to have secure mechanisms and to make use of the secure mechanisms. Given his decreased faith in companies, despite using more tools for security, he has less confidence in his ability to protect himself.

P005

P005 was affected by the Equifax breach. She is an Asian woman, with a graduate degree, between 35 and 44 years of age. Her approximate annual household income is $150,000 - 199,999. Her face-to face interview took place on March 6th, 2019.

P005's financial activity online didn't change due to the breach. She still checks her back account online, deposits checks, pays bills, and does a little stock trading. Even before the breach she knew that giving data to financial institutions that operate online could be risky. To her, every business interaction poses a risk "even just from the basic employee taking your information". However, she made an effort to protect her data by checking for https or secure locks on websites, avoiding public wifi, and generally keeping eye on her accounts. However, she acknowledges that all these efforts are weighed against their convenience. "Just because when you're busy, your life is busy. You've got kids running back and forth. You have to weigh that risk of what you want to be able to manage, so I just take it as one of the things that I know it might happen, might affect me. I know like my debit card have occasionally been tagged for fraudulent charges. I just had to minimize [risk]."

She felt before and after the breach that individuals and organizations are both motivated by their own self-interest, which can sometimes align with the interest of others. Before the breach, she had a high level of trust in Equifax, "because of their reputation. And, because we live in a litigious society that if there was very well known, documented negligence on their part, people would sue. I assumed that they can sue. So most organizations want to avoid lawsuits; so that keeps them on the straight and narrow."

The breach caused P005 to realize that all her data was online. “I didn't really think about it. I just. I don't know. It's like one those things where you just didn't quite realize all that information's online.” After that realization, she reported feeling as though she had no control over her information. “I can only control what I have access to right? So, saving my information into a website, that is my choice. That is something that I could control. I don't know that I've ever seen where a bank says you can opt out of having your information online. So there's no opt out there.”

This lack of control and the unavoidability of Equifax’s possession of her data distressed her. “So [I’m] not happy, right? I'm not happy that they are major agency. I don't have a choice in where my information is stored with them. And so, they should have the highest-level security, the best cyber experts. They should do frequent testing and monitoring of their systems enough to be able to catch anything like this because we don't have a choice there.”

P005 said she “want[s] to believe that organizations like that understand their responsibility to our information.” But she has concerns that “organizations cut a little too much in terms of cyber expertise, because they get complacent…. They don't innovate their practices.” This concern is exacerbated by her view that hackers are “very savvy.” In her view, hackers “find creative ways in and out. And if you don't have a top notch and creative cyber security team, who is staying abreast of everything going on, your organization will at some point be breached.”

These days she believes that Equifax is “probably being very vigilant and probably will be for the next few years.” “I think they are probably gonna be vigilant for a while and for now. But I don't trust them to keep my information safe. But I don't have much of a choice either."

She concluded her interview by discussing our increasing relance on digital spaces. "Now we live in a very digital world, so that's just a risk that we have. And I wish there was other ways. I don't...I like my digital world. I don't want to go off the grid, so to speak. I think there's some situations, I mean, there's definitely ways that you can't go off the grid. Right? Credit reporting agencies have your information. Banks have your information. We don't live in a cash only world."

P006

P006 was affected by the Equifax breach. He is a white man between 35-44 years of age, who attended college. He has an approximate household income of $100,000 - $149,999. His prior work experience includes working in real estate, military service in the army, and work in a security field. His phone interview took place on March 4, 2019.

P006 describes himself as “fairly security conscious.” His online activity reflects that. His only online financial transactions are purchases. For that purpose, he has two credit cards selected for their fraud protection. If he asses a site as risker he uses “PayPal to a credit card.”

When P006 discusses his security behaviors online, some pride is evident. “I'm one of the only people I know that Facebook's visual tagging does not work.” He enjoys creating amusing and difficult to crack passwords. The Equifax breach made him “mad” and “incredibly frustrating, because that's not a voluntary service.” “That's one that they are given [my data] by others for me having the privileged to take part in economy”

He sees giving information to financial companies that operate online as “nightmarishly awful in all cases.” From his work in real estate, he was very familiar with Equifax’s data collection practices even prior to the breach. He argues that with their current business model, true security would be impossible. He sees this mandatoriness as a risk that cannot be mitigated by the individual. “There's a handful of these that there's nothing you can do about it. I mean, like, from an individual citizen standpoint.” Given the steps he takes to control his data security as an individual, the lack of recourse adds to his frustration. “It's extremely, extremely frustrating, because there's no way to remove your data from Equifax. It's not like you can send them an email or a letter, even you know, like, sue them to remove all your information which they have without your permission.” “There wasn't even someone I could send a snippy e-mail to.”

“I don't think their security problems are lack of ability. I think they are lack of interest and allocation of resources. You know, anybody has the ability to absolutely one hundred percent lock down data by not putting it online. You know, it's one hundred percent in all cases to that have the ability. Now, and I'm saying this for research purposes, not because it's not really obvious to you, but we all choose the amount of access to that data based on convenience for our needs. And for the convenience for their needs for their business model they have to give incredible access to it. Because people that they have no way of verifying if they know me or not access my data through their service. For eleven dollars.”

P006’s perspective that anyone can protect data by taking it offline is unique among are participants, who otherwise assume that online financial operations are inevitable in the modern era. He sees Equifax’s business model as logical given their profit motive, but incapable of providing security. He further believes that “They are going to be wanting to protect the financial companies that use their service, not the product.” Despite this sense of inevitable poor data guardianship on the part of Equifax, recent breaches did trigger changes to his behavior. “I have changed the way I do passwords. I've started using grammatically correct sentences.” He also signed up for a notification service that alerts him when his information appears on the dark web. Otherwise, he has accepted these online security risks as unavoidable and exerts his protective energy in the areas, such as information rationing, where he feels they would be most productive.

P007

P007 was affected by both the Equifax and Facebook data breaches. Her data is included in the Equifax data set, but all her responses will be summarized here. She is a white woman, between 65 and 74 years of age, who holds a bachelor’s degree. Her approximate annual household income is $200,000 or above. Her face-to-face interview took place on March 15, 2019.

P007 manages most of her finances online, including banking online, credit cards, investments, and retirement accounts. Before the Equifax data breach, she used passwords that were based on fairly public information such as names. Due to the Equifax breach, she changed her passwords to “a series of letters, number, and special characters.” She also now pays attention to her local network: “I do watch who, if anybody is trying to ping my home network. Because you can tell what devices are signed on. So, I do watch that for a breach.” She sees herself as an above average user when it comes to security but expects “Equifax would have more ability than me. They should. If they don't have somebody that's smarter than me on their IT security, then shame on them.”

Before the Equifax data breach, P007 “figured companies had safe data.” Partly due to the security measures in her own workplace, she views sound data protection as a core business function. She expected Equifax to have excellent security. “I think they should have had a strong IT department with all the sensitive data they had. They should have had secure servers. They should have had back up information.” Based on the amount and sensitivity of the data held by Equifax, she compares them to a bank. “They were kind of like a bank. I trust that a bank is going to have a safe. Could somebody blow up the building and get into the safe? Sure. But could they really? How many people walk around with a ton of dynamite?" "They should have been protecting their own stuff. That's their business. So, in order for them to make money and be trusted they should have had their safe locked."

P007's view of the Facebook breach is somewhat different. She had been a fairly active user of social media, checking regularly for pictures of children in her family and seeing what family members were up to. Even before the breach, she viewed these platforms with caution. "I think it is completely risky to give data to social media companies. I wouldn't put my home address on there. I don't like them tracking me. I turn that off." Based on experiences in her workplace, she was aware of Facebook's extensive data collection. Nevertheless, the data compromise surprised her, because "I didn't think they would sell the data, because they wouldn't share it with companies they had apps with. So why would they just outright sell their database? Which is what they are doing." She knew that Facebook collected data but did not expect them to sell access to what she interpreted as "their valuable asset."

To protect herself and her data on social, P007 primarily relied on limited what data she provided, prior to the breach. After the breach, she changed her privacy settings. She no longer plays games on social media, nor will she "click forward within the Facebook app." She expressed frustration that "Facebook has gotten away from the purpose that I liked it for, because I could go and just look at the family. And now there's so much crud that it's not even worth getting on."

To her, the most upsetting aspect of the Facebook breach was not their giving out access to users' data, but instead what they have allowed onto their platform. "To me, that's

Facebook's biggest thing that they allowed people--- they didn't investigate who was entering their site and what was being posted. And that to me is a bigger breach than selling the information. Because, they allowed a foreign government to influence our election, because they didn't monitor their own business. Now that's...that I think they should truly be held accountable for. They probably had the right to sell our information, and we were just stupid and didn't know it. But the other one. They're just not even monitoring what's on their site. And they could definitely do that. They have the ability. 100%. They were greedy. You know, they were making money, and they were sloppy."

P008

P008 was affected by the Equifax breach. He is a white man, between 35-44 years of age, who holds a bachelor's degree. His approximate annual household income is $75,000 - $99,999. His face-to-face interview took place on March 22, 2019.

P008's routine financial online activities include Ebay, Paypal, and, less frequently, investment accounts. He also makes online purchases, usually through Amazon, about once a week. In terms of personal guardianship behaviors, he changes his passwords when prompted. After the breach, he froze his credit.

P008 does not see giving data to financial companies that operate online as particularly risky. Before the breach, he felt that Equifax "probably did a great job of what they were doing." This view was mainly due to the fact that since he "never had a problem with them" there was no reason to view them otherwise. "Why would you think they were not on top of their problem?"

The Equifax breach affected P008's view "to some extent," because protecting data "should be one of their biggest priorities and they failed it." However, this did not change his online activities at all. He feels pretty confident in his ability to protect his data online and considers himself an average user in that respect. One of the reasons for his lack of strong concern is: "I'm probably not as big a target as some place like [Equifax], so I don't see myself as in as big a danger in compromised." He trusts Equifax a little less, but mostly believes they are willing to protect his data, but he doubts their ability to do so a bit: "I think they want to it's just they lost the ball on that one."

P008 thinks that individuals are generally out for their own self-interest but believes that this makes them better data guardians than large companies. "I think individuals are gonna have a lot more motive for protecting your things than a company would. It affects an individual. Impact is greater on an individual than it is, I think, on a company."

P008 believes that Equifax is likely to be protecting his data "better than they were in the past," but acknowledges that he is only assuming that they "scrambled to fix their problems." Today he believes: "it was in their interest to protect the data and they fell down on the job." Overall, the breach had a fairly small effect on his beliefs and routines.

P009

P009 was affected by the Equifax breach. He is a white man, between 55 – 64 years of age, who holds an associate degree or professional certification. His approximate annual household income is $200,000 or more. His face-to-face interview took place on March 27, 2019.

P009's routine online financial activities include online banking, credit cards, and purchasing. He has alerts to notify him about purchasing and account balances. He describes himself as "paranoid about giving my data to people" and feels that giving data to financial companies that operate online is risky.

Prior to the breach, he did not consider the risk that credit reporting agencies could pose. "Before, I never really thought about that data from the credit reporting agencies being out .... It's kind of like the government, you never think about how that information might get breached or put out to other folks that may not be honest with that information."

P009 describes the Equifax breach as "an eye-opener" that made him realize "your data is out there, so you need to protect what you can." After the breach, he is even more reluctant to give out information online. He says that he "lost trust in not only Equifax, but the other credit reporting agencies too." The breach made him feel as though he didn't have any control over them having that information." This lack of control "is one of the reasons why [he] took steps that they suggested that if your data was possibly breached you may want to lock your credit reporting, so [he] did that."

P009 generally feels that individuals are out for their own interests. When it comes to Equifax, he says: "I just try to do what I can to hold them accountable, which is not much. Other than do my part, which was get on their site and ask for the data to be locked, and stuff like that. Then they followed up with a letter and communication saying they had done that. That's about all I felt like I could do.”

In terms of Equifax having improve security, P009 has hope, but no trust. “Hopefully [they are protecting data] a little better than they were before. But do I think they're going to ace it? No. Will it happen again? Probably. He is, post-breach, even more hesitant “to give out things like social security number, stuff like that, too much personal data.” Social security numbers, for example, are “probably a little more than they need to know.” He also now looks for the address bar lock indicating secure sites, and he tries “to go to sites where people are generally using, not some site that is not frequented by lots of folks.”

Despite describing himself as “not a fan of big government,” he said “that's the case where regulation could be good…. It costs them dollars to obviously protect that data, and maybe they were trying to not spend those dollars. Therefore, maybe if they'd been a little more protective, and we'd had some regulations in place, then they would have had to spend those dollars. “

P010

P010 was affected by the Equifax breach. He is a British, white man, who has resided in the US for many years. He is between 55-64 years of age and holds a bachelor's degree. He has over forty years of experience in the IT field. He declined to provide income information. His face-to-face interview took place on March 28, 2019.

P010 describes his online financial activities thusly: "banking and looking at what's left of my investments, and shopping anyway." He currently uses a VPN for all site except Amazon, which throttles VPN connections. He also encrypts whatever data he can. After the breach, he signed up for credit monitoring.

Pp10 says that "anything online is risky," but he was still surprised by the Equifax breach. And, in fact, reports thinking that his perspective before the breach was that Equifax could provide protection. He acknowledges some cognitive dissonance in this view: "Even though I've spent so long work in the industry and know that they don't."

P010 "lost faith" in Equifax after the breach. He says that "if it happens once it can happen again." While he considers himself to have an above average ability to protect his data, He notes that he has no "control over any of the credit agencies having all [his] information." He adds that "you've got to rely on companies like that to be solid and in control." He also expressed frustration with how long it took for Equifax to notify users of the breach: "I get annoyed when companies have a breach and wait a few months to tell you."

As for how well Equifax is doing now, he thinks they will have improved their security about "90 something percent."

P011

P011 was affected by both the Equifax and Facebook breaches. His information is included in the Equifax analysis. His interview was unique in format in that post-breach questions regarding both cases were asked consecutively, followed by pre-breach questions about both cases. This structure lead to the need for consistent clarification and was therefore abandoned in future interviews. P011 is a mixed-race man between 35-44 years of age, who has attended some college. His approximate annual household income is $50,000 - $74,999. He works for the University of Tennessee Health Science Center as an IT security analyst.

P011's online financial activities include banking, online billpay, and purchases. His personal guardianship behaviors include the use of two-factor authentication and a password manager. He views giving data to financial companies that operate online as "very risky." This is a marked change from before the breach when he "expected [Equifax to have a great precaution against [breaches]."

P001's initial reaction to the Equifax breach was "Oh, here we are. Another breach." He says he did not trust Equifax before and does not trust them now. Though, since the breach, he expects Equifax to "remediate and probably a year later they'll be improved." His generally expectation is that people are about 50/50 benevolent versus self-motivated. Perhaps more importantly, when it comes to security, he feels that "usually everybody hears about [the breach] for a week and then goes back to their life and they don't think anything else." Companies, he says, are motivated "to watch out for my data otherwise they lose trust," especially after a breach when "their stock price can't take another hit."

The Equifax breach did not change his protective behaviors much, but he has added a password manager due to improvements in the availability of those technologies.

P011's online social media activities are limited to scrolling through Facebook and making occasional comments. His personal guardianship behaviors include not posting geolocation data and not posting vacation pictures while actually on vacation. In general, since the Facebook breach he tries to post on Facebook less. Facebook prompted him to reset his password, which he did. He also checked his privacy settings.

Since Facebook is a free service, he sees himself as their product. Both before and after the breach he says he "had zero trust" in Facebook as a data guardian. Given the sheer volume of data Facebook manages, he feels that they cannot protect user data. Between user behavior and technical issues, he argues that such protection would be impossible. "In no way are they actually able to protect all of your data like you would think." Even before the Facebook breach, he "never really expected them to do a great job at [protecting data]." He argues that they cannot provide security, because they are likely to be targeted by all types of attackers. "They're a big target for everything, hackers, nation states, and everything else."

Even with the best technical security possible, P011 feels that "if people don't take privacy in their own hands, especially when it comes to social media and Facebook, it's not going to do any good." That said, he doesn't believe that Facebook is providing good technical security. Instead he thinks "they have a better PR firm and probably whatever else they add but it's definitely going to come down to PR." He sees future breaches as "pretty much a fact of life at this point."

P012

P012 experienced the Equifax breach. He is a white man, between 35 – 44 years of age, who attended some graduate school. His approximate annual household income is $200,000 or more. He has a poly-sci background. His phone interview took place on March 28, 2019.

P012's online financial activities include checking his bank account and investments, online billpay, purchases through Apple Pay or Amazon, and monthly checking of his credit reports. His personal guardianship behaviors include using two-factor authentication, using different passwords, only accessing sites through their apps, using VPNs when on public Wi-Fi, never using public computers, active credit monitoring, and frozen credit.

When P012 was notified of the Equifax breach he was surprised, because at the time he saw Equifax as "very good." But when it happened, he also saw the breach as "kind of expected." He describes his view of online risk as "I guess my view is that it's not whether or not your data will be taken or will you be compromised in some way. It's how quickly you recognize that you've been compromised." He sees financial activity online as less risky that social media, but still risky.

Regulations, in P012's view, "don't necessarily make it less risky." He sees regulatory compliance as "maybe a cop-out." "If they're complying with the regulation and they've passed their audit, they don't necessarily have to go above and beyond. So I guess it's, I have kind of cynical view towards institutions I suppose, and the way they protect people's data." "As soon as you regulate, you put a target for them to hit. If they're hitting that target, they don't have to spend money going above and beyond the target."

P012 sees Equifax as just like other financial institutions, though he would like to "hold them to a higher standard, because of the power that they have over an individual's ability to obtain credit." He sees his own ability to protect his data online as above average. Since the breach, he believes that he has "a greater ability to protect [his] information that Equifax does." He believes that "most of what they're doing is probably superficial." P012 says that he hasn't changed much in terms of online routines, since the breach. He uses VPNs a little more frequently and checks his credit a bit more often, but overall, he sees his routines as the same. What has changed is his level of caution and skepticism. He is "more aware of the potential of a theft." In the past he says, "I perceived Equifax as capable of protecting my data and felt like they were a beacon in the data protection area I guess." The breach shook that trust and the time Equifax took to report the breach to users disappointed him. "They didn't immediately notify people. They found out they'd been breached, they sat on it, they tried to fix it, they tried to sweep it under the rug, instead of just owning it."

Now, P012 says "I guess just my general outlook is that your data is available. People can access it. It's how quickly you identify that you've been compromised that matters. It's not whether or not you'll be compromised." "And there's humans, there's wires, you can plug things together, there's the ability to compromise is there. The desire to compromise is there. People want to steal stuff. It's there. So I mean, I just think it's a reality. And I think it's taken society a long time to, I guess not really a long time, I'd say about 20 years, to understand that it is a reality. Your data will be compromised. Things will get hacked. And just to accept it."

P013

P013 experienced the Equifax breach. She is an African American woman, between 45-54 years of age, who holds a Graduate or Professional Degree. She runs her own business, and her approximate annual household income is $35,000 to $49,999. Her phone interview took place on April 4, 2019.

P013's online financial activities are limited to banking, QuickBooks, public trading, and purchasing. Her personal guardianship behaviors include "whatever those strange requirements are to create a password." She vigilantly checks her accounts for fraudulent charges and has notices set for purchases at the lowest threshold available.

P013 had a very consistent message thorough her interview. She does not trust Equifax. This is her story:

"On my credit report, if you go back more than the 10 years until it rolls off, it looks as if my house has been in foreclosure. It has never, ever, ever been in foreclosure. Not ever. There are specific legal things that must occur for you to actually go into foreclosure. Chase, who is now my current mortgage holder, now, I don't think they would be if I'd gone into foreclosure. They were my mortgage holder then, too, had me reported as if going into foreclosure on a second mortgage, which I no longer have. But no matter how many times I present to Equifax: "this did not occur, there is no legal ... There's nothing. No notification, no nothing on my end, there's nothing in the courts that would say that this is true." Every single time, Chase would say, "Oh, it is true." Without any proof whatsoever. And that stayed ... Well, technically it's not on your credit report because they only go back 10 years, but the point is I had to wait like three years for it to roll off my credit report for something that never happened, because a big company said, "Oh, yes it did," without any verification of that at all. This is why I don't trust Equifax, which is why I believe that they're bought.”

Based on this prior experience of Equifax, she has absolutely no trust in them as a data guardian or user advocate. “Well, the corporation's job is to maximize shareholder wealth, so I'll think that Equifax will protect data only as much as it lines their balance sheet, but they do not ... Their balance sheet grows better by not always protecting my data. They may do it 99% of the time, but it's the 1% that creates the panic that then allows them to benefit from the panic. That's what I believe about Equifax and all the other public companies, public credit unions.”

Due to her lack of trust and her beliefs about Equifax’s business model, P013 does not rely on the security products provided by them. ““‘Because my belief in that is, again, it's there to create a false sense of security to then break that false sense of security to then sell you LifeLock super. They'll supersize it. It never ends.” Since the breach, she is more cautious about which websites she purchases from. “Well, I used to assume that any website was probably a safe website if it looked legitimate and I wanted to buy something, say some flowers. Flowers are a good example. You can call 1-800-Flowers and send the information anywhere, but I would try to ... I'd just look for the best price versus looking at a website and going, ‘How is this going to affect my security if I go through this smaller website?’ The pages and stuff or the pictures are not quite aligned with the words, because they probably did it themselves. It makes me pay closer attention to that, and I'd rather pay a few more dollars just to go to someplace that I know the reputation is there.”

P013 reminisces fondly about the days before Equifax became a publicly traded firm.

“Well, you know, back a long, long time ago in the land of no gray hair. You were able to go to the credit bureau on Summer and pull your credit report, people were nice to you, they would tell you what was on it. It made sense, all the stuff matched up, and it was really a matter of providing a service to the consumer, the person in front of you. I no longer feel that. Equifax, and all the public credit bureau companies, are here to create and to allow certain amount of breaches to benefit their own good. I firmly believe that. I think that's how they make their money.”

P013 is very aware of the power differential that the current system creates, but her concerns go further than Equifax, credit bureaus, and the like. “I just feel like we're being led. We're going to go into a digital world whether you want to be there or not, and it remains to be seen if that'll work to everybody's benefit or not. High technology, whether you want it or not. Certain amount of technology I fully support, but I don't need all the extra bells and whistles. My life was fine without them…. You don't have to do all of it to have a full life, but I feel like we're being pushed in a direction where the highest technology is what you're going to have to have, whether you want it or not. And if you're not within certain income levels, you're just going to be left out. So, you won't even be able to access what it is you need.”

P014

P014 was aware of the Facebook breach. She is a white woman, between the ages of 35-44, with a graduate or professional degree. Her reported annual household income is $75,000 - $99,999. Her phone interview took place on April 10, 2019.

Today, P004’s online activities on social media are mainly limited to Facebook, Google Hangouts, and an online journal accessible by a few close friends. Her routine personal guardianship behaviors include randomize passwords which she changes monthly. She describes herself as “incredibly careful about personal information.” She supports this with examples: “I share very little personal information online, and that includes things like my birthday. Not the entire date even, but just like the month and the day. I don't want anybody to know my mother's name, regular or maiden. I don't want anybody to have my address information. I don't put anything in to do with like cities that I belong into. I try to keep personal information as private as absolutely possible.”

The Facebook data breach acted as a trigger moment for P014, resulting in substantial changes to her behaviors. She now thinks sharing data online is “extremely” risky. “It's very strange, because I think it's something that we knew, we being society, I think we knew that it wasn't safe, but then there was this realization of exactly how unsafe that could be. I ended up doing a credit freeze. My credit is still frozen. It was something where I kind of avoided putting personal, like emotional information out there very much, except for on my journal, but this is when I started saying, ‘Let's not mention birthdays, let's not mention any of that.’ That's also where I started limiting purchases.”

As this quote indicates, the Facebook breach affected not only her social media habits, but also her financial ones. “I try to pay online only for places that I feel confident with, so I don't... I'm careful about my purchases and where I purchase and whom I make purchases through. I have a PayPal account that gets used, primarily for anything that seems like a small business, because I don't want to put my data through them directly. Then paying bills and that kind of thing. Amazon gets used for whatever I can't buy locally. But I'm very careful about where I'm going to put that information."

Prior to the breach, P014 saw Facebook as a product, like a game or other software. "I figured that all social media platforms were doing their one thing, and that was the thing they were doing, and they were all basically doing it the same way. In the same way that I would download a computer game, and the download goes kind of the same way, and then I play the game, and then I can take it off the computer when I want to. I felt like they were much more basic structures than they are."

The breach changed P014's feelings about Facebook and the structures in which it operates. "I feel that there's no actual oversight, and there were no— I don't know of any penalties or anything, and I don't know that they've lost that many customers, and so I feel like there's not enough— Why would they bother doing anything if they can still continue running their business and everything is fine?" This distrust has resulted in a decision to leave Facebook entirely. "I am very angry, both at myself and at them, for the lack of knowledge that I had to begin with about how much data was being shared. I still don't have a really full understanding of what they're taking, and that feels like a pretty huge violation, which is again why I'm leaving [Facebook], so surprise, which I have interestingly not announced on Facebook. It can hear me now though. It's going, "Oh no."

P014 provided a vivid metaphor for the difference between what she thought Facebook was doing in terms of data collection and guardianship and how she now perceives them. This is her explanation:

It's the difference between going to a zoo, and then going into the safari, right? I'm signing up for the zoo, where it's all contained and comfortable, and then finding out that there's actually no walls and nobody has been given any food, and so everybody's super hungry, and enjoy your run from the lions!

P015

P015 was aware of the Facebook breach and affected by the Equifax breach. He is a white male, between 35-44 years of age, who holds a bachelor's degree. His approximate annual household income is between $35,000 to $49,999. His face-to-face interview regarding the Facebook breach took place on April 11, 2019; he was not interviewed about his experiences regarding the Equifax breach.

P015's has been a Facebook user, since the site was restricted to individuals attending college. His social media activities online currently include Twitter and Facebook. In the past, he was also an active Reddit user, but he has stopped frequenting Reddit for reasons unrelated to the Facebook breach. His routine safety precautions include using trusted networks and privacy settings. He considers himself an average user in terms of information security ability.

The Facebook beach came to P014's attention through news sites and social media posts. His immediate response was "Well, shit, I guess, you know, I'm one of many so I guess I didn't feel as personally violated since I'm like, well they're violating everyone so." He equates the breach to "doing their research for free, since they want to know rather than paying people to answer all these questions about their personal beliefs by posting or commenting and all that, I'm just giving the data for free." He says he doesn't view Facebook as risky, because he never viewed it as private to begin with. "I wouldn't call it risky since it's just sort of like, I mean, I guess it definitely didn't feel like that this is like my own little place to post my own opinions, and they are limited to whoever's my friends on there."

The Facebook breach did change his perspective somewhat. It “definitely made my opinions feel more commodified.” But this feeling of commodification didn’t begin with the breach; this was a feeling that P015 had already begun to have about the site. Around the time of the breach he stopped using the app… it was about the same time. I think it was just the growing distrust of Facebook and growing distrust of me being addicted to it. I stopped using the app, and I did go in and check my privacy settings, too.”

The Facebook breach also changed P015’s view of the value of seemingly innocuous data. “Again, I guess I really underestimated what value that data might have to others. Since, like I said before, it felt like a lot ... there was not impediment to share your thoughts and opinions about things because you're like, ‘Well, everybody's doing this right now, so it's not very—’ Again, it's like, "Well of course, that's why it's valuable." But then it's like, "Who would want to have to sift through all of that? But, again, like I said, it's not sifting through it once you remove the personal, the people out of it, it becomes more about just the information, the data then it's easier to violate people that way.”

After the Facebook breach, P015 stopped using the Facebook app and made an effort to reduce his Facebook use. His attempt to curb his Facebook use was not, in his mind, directly linked to the breach, but rather to an overall sense that was that checking Facebook had become an automatic reaction to using his phone: “you know, I wake up and check the time on my phone, then immediately my thumbs choose to open up Facebook… Then I'm like, ‘No thumbs, we don't need to look to Facebook right now.’” Results of this effort have been mixed; during our interview, he jokes that Facebook was open on the computer behind us.

One change P015 does attribute to the breach is a decrease in posting. “[The breach] just makes me less likely to want to participate in Facebook. I think I read more Facebook than I am writing on Facebook than I used to is probably what I would say is the biggest change.”

P016

P016 was aware of the Facebook breach. She is a white woman, between 35-44 years of age, who holds a graduate or professional degree. Her approximate annual household income is $50,000 - $74,999. Her phone interview took place on April 14, 2019.

In a typical day, P016 skims Facebook and Instagram for news of her friends. In terms of current personal guardianship behaviors, she tries not to link accounts to Facebook. She also restricts the information she puts online “both in terms of the statuses [she posts] and how specific they are to my location and specific information about me and my life like pets names, addresses.” She also restricts access to her posts and information using the site’s privacy controls.

P016 learned about the Facebook breach on the news. The breach made her “aware of how important the seemingly unimportant stuff was like access to my birthdate or places that I had been or the town that I live in because those are security questions that people ask for, for a lot of other sites.” Before the breach, she was aware that “we're kind of living in an age where we know that there is a risk to the information that we provide.” After the breach, though, she felt very strongly that “these people are not protecting or are not capable of protecting our information in a day and age when cyber warfare is becoming as predominant. She went on to explain, “It made me feel like the company itself, that whether or not their intention is to protect my data and I question whether or not their intention really is to protect my data, but it made me aware of the fact that they are incapable of doing so.” P016 is very scared by her belief that Facebook cannot protect the data of its “two billion or however many users across the world.” This fear causes her to “kind of shut down online information as much as I can.”

The manner in which Facebook dealt with the breach also affected P016’s view of the firm as a data guardian. “I feel like the number of data breaches that they have had and the way that they dealt with the data breach being that ... being that there wasn't a lot of information provided to the users about it. They didn't address it very publicly and then I feel like when people tried to address it publicly, especially on Facebook, some of those accounts were shut down and the posts were shut down. So, I felt like Facebook was trying to kind of cover up the fact that there was a data breach in the first place. So, it makes me feel like not only are they not capable of protecting my data, but they also don't want me to have the tools and the information to know that I even need to protect myself.”

Before the breach, P016 thought of Facebook positively. “I very much kind of lumped Facebook and Google and a lot of these major organizations into the same category and …. as this progressive new age of companies that were willing to go the extra distance to make sure that they protected my security and that they had my own best interests at heart because they kind of "got it". We were part of this similar generation with similar beliefs and I put them separate for some reason in my head from a lot of the financial institutions because I assume that they don't have my best interests at heart, but these other companies I assume are part of this next wave and next gen that would fight against governments getting access to our information and would go the extra mile to protect us. And I don't feel that now.”

P016 feels a good bit of disillusionment since “I had previously used these platforms as ways of engaging with my friends and had not realized the magnitude of the information that I was sharing and what these platforms could be used for and how they could affect events on such a grand stage. And it ... yeah and it leads me to back away from all of it, which I feel like can be very isolating in today's day and age. So this thing that I was using to engage with people from distances is now fraught with danger, which I think leads me to feel more isolated in a world where I would otherwise engage more regularly."

Isolation in the absence of alternatives to Facebook is only part of the negative's P016 is now experiencing. She is also wrestling with the ramifications of the breach for herself and others. "It's terrifying. It is absolutely terrifying to know that the data that they can gather from us as individuals can lead to affecting national elections or killings in Myanmar or social uprisings in countries."

P017

P017 was aware of the Facebook beach and was affected by the Equifax breach. He is a white man, between 35-44, who holds a graduate or professional degree. He works for the US Navy. His approximate annual household income is $35,000 to $49,999. His phone interview regarding the Facebook breach took place on April 15, 2019; he was not interviewed regarding the Equifax breach.

P017 describes his online routine thusly: “On a typical day I will say that my activity consists of maybe reading, like RSS feeds with articles, which will often have or be prompted by tweets. So I will click and view those tweets generally without being logged into a Twitter account. Yeah. More rarely I will get a link to a Facebook something, which I am lately not following those links, yeah, I think in part driven by Facebook's more aggressively making me log in to engage with those. Let's see, other social media. I'll check Instagram usually on my phone maybe every other day or so.”

P017’s personal guardianship behaviors include two-factor authentication, unique passwords, and limited posting. He also has automatic alerts for logins turned on to ensure he will know is someone else accesses his accounts.

P017 considered the Facebook breach simply confirmatory. “I think by the time this breach hit the news, I already didn't trust Facebook to keep my information controlled in a fashion I could understand. So having my account compromised out there meant that somebody at Facebook didn't approve of could access my information, but plenty of people that Facebook did approve of, I'm under the impression, could already get my information.” He did not trust Facebook before the breach, and the breach confirmed that stance.

P017 feels that he has a significantly above average ability to protect his data online: “I'll say maybe, let's call it two-and-a-half sigma above the mean.” He does not see his own ability to protect his data as coupled with Facebook’s role as a data guardian for the simple reason that he does not see Facebook as a data guardian. He views Facebook as a source of risk, rather than a source of risk mitigation. P017 does believe that Facebook has made some changes to their security, since the breach. But he does not expect these changes to meaningfully affect the security they provide.

P017 no longer posts often on Facebook. Before the breach, he “had already stepped back [from Facebook], and [he] didn't feel the need to step back further.” However, for him, as for many participants, his presence on Facebook is not entirely his to control. “So my fiancé loves to post pictures of us on Facebook, and I make it clear that I have no secrets and she should use Facebook as she wants. But I don't love it, and I don't know how to decouple that. I don't know whether that is because of Facebook just as a social force and how much of it is concerns about the privacy. Yeah. Although, I guess I am, due to some other unrelated parts of my life, I am aware that everything that she posts, or I am under the impression that everything she posts, has been available to anybody who has more than a passing interest in the connect-the-dots picture of my life.” This quandary of balancing social responsibility to others with one’s own desire for privacy is a common and difficult calculus for several of our Facebook breach participants.

P018

P018 was aware of the Facebook breach and affected by the Equifax breach. She is a white woman, between 65-74 years of age, with a high school education. Her approximant annual household income is $100,000 - $149,999. Her face-to-face interview regarding the Facebook breach and Equifax breaches took place on April 15, 2019. Her data is included in the Facebook case data set.

P018's online social media activity is limited to Facebook and Instagram, which she checks daily. Her protective behaviors include using privacy settings to limit who she allows to access her accounts. She first heard about the Facebook breach on the news. The breach made her feel that social media was a little riskier than she had previously though. It also changed her view of Facebook as a guardian. Before the breach she viewed Facebook as trustworthy. She thought "they had the technology set into place that it would not be penetrated." She felt, after the breach, that protecting her data was not a high priority for Facebook. She realized at that time that she didn't really understand the risks posed by social media, nor what steps she should take to protect herself.

The Facebook and Equifax breaches are somewhat intertwined in P018's mind. She remembers changing her password and checking her privacy settings on Facebook, but otherwise most of her revised guardianship behaviors have to do with Equifax and financial routines. She doesn't know whether or not her social media data will be protected now. She feels that Facebook only protects data when protecting that data is financially beneficial to their bottom line. Since the Facebook breach, P018 gets on Facebook less often. She is more reluctant to click through links on Facebook. She also doesn't accept friend requests as readily.

In P018's view, Facebook failed in their social responsibility. "I think that there are people out there who are very vulnerable and that [Facebook has] a social obligation to protect them as a company."

P018 seems much more invested in the Equifax breach. Her online financial activity includes banking, bill pay, credit cards, investments, and purchases. Her personal guardianship behaviors have changed since the breach. Once she was notified by Equifax that her data had been compromised, she signed up for LifeLock, froze her credit, stopped accessing financial sites anywhere but at home, stopped accessing investments online at all, and began to check her credit card purchases regularly and contest any suspicious looking charges.

The Equifax breach caused P018 to feel that sharing financial data online was riskier than she had though. It also reduced her confidence in Equifax as a guardian. Her self-confidence increased at the same time, because she identified specific steps that she could take to make her financial data more secure. With Equifax, she feels a certain partnership: "I think there is more of a partnership. Like I have a responsibility to protect my data in partnering with them in the ways to that they can help assist me in protecting my data." She is not sure if Equifax is protecting her data any better today than before the breach, but she is thinks that she is protecting it better, which seems to provide her with some comfort or confidence.

P018 draws a distinction between Equifax and Facebook as protective entities. She feels that it benefits Equifax to keep data secure, while people will use Facebook whether their data is secure or now.

P019

P019 was aware of the Facebook breach. They are a Caucasian and American Indian/Alaskan Native, non-binary person with a disability. They are between 18-24 years of age, attended high school, and have an approximate annual household income of less than $24,000. They have prior of experience of threats and harassment on social media platforms, which may have affected their experience of this recent breach event. Their face-to-face interview took place on April 4th, 2019.

P019 uses Facebook “a lot more than [they] should.” They use Instagram “quite a bit,” which is also owned by Facebook. They use YouTube “hours a day” in the background. They have reduced their use of Tumblr, since it was bought by Yahoo. They have a twitter and reddit accounts, but these are not part of their regular routine. They rely on Facebook Messenger as their primary means of communication, since they have no phone at present. P019’s personal guardianship behaviors include setting all accounts to private when created, physically covering their webcam, restricting what they discuss online or on devices that can go online, and limiting content stored on such devices.

P019 began our interview by raising an issue that ran throughout our discussion. They feel violated by the auto-sharing of their online activities; examples of this include the Facebook recent activity sidebar or Spotify/Facebook widget that shows your friend’s listening behavior. The streaming update of one’s activities, entertainment use, and other behaviors to all one’s friends recurred throughout P019’s interview as evidence that Facebook had gone beyond tracking one’s behavior and into consolidating and mapping that behavior for the consumption of other without asking for consent. They described the different between the former and the latter thusly: “There is a difference in my brain almost between I collected your shopping data that you bought orange juice last week, and I went around and filmed you in the store."

Lack of control over their data on the internet is very concerning to P019. They see the data breach and the information about Facebook's data collection that became public as a result of the data breach as evidence that Facebook is "like this giant, monolithic, I guess mega corp. [Prior to the breach,] I knew they had the data on me, and I knew that there was things that they were selling to advertisers obviously….[But], it felt like we were just commodity not being exploited and ringed out." Prior to the breach they believed that Facebook was "selling [data] to advertisers and people who were claiming to be businesses, but they probably didn't just have it out there." They viewed Facebook as provided a forum for social interaction in exchange for the use of our data. After the breach, their assessment changed. "Like there's the added layer now of, 'Oh, great. I guess Facebook isn't even doing anything,' because before it was, 'Oh, people are always going to be out to get my stuff,' and now it's, 'People are going to be out to get my stuff and the place where my stuff is kept is not very secure and they don't particularly care about that.'"

P019 describes the current environment as dystopian, particularly for poor individuals who cannot afford communication options other than Facebook. "I've always kind of had this weird feeling of being watched, but that may have been influence from prior internet experience and so I guess it didn't shift it that much but it more made me feel like instead of, oh I'm being watched it is everyone is being watched. I feel more like just the environment we live in is being weaponized against us, things that we pretty much can't live without, and a lot of people who are in my situation use because it's the only option is just...Gosh. It just feels more dystopian I guess is the word. It feels like this shouldn't be a thing, it shouldn't be allowed but it is and not really we can't do anything about it but there's not really anything that one specific person can do and it's just like, "Oh, I don't have a phone right now. I have to use Facebook Messenger for everything I'm going to do."

Facebook’s lack of guardianship “just adds this other layer of worry, of I've got to be extra vigilant now to make sure that the people who are going to hurt me don't hurt me because they have more access.” They seem themselves as below average in their ability to protect their data online. “Given my circumstance I'd say below average because so many people know so many things about me from way back when I knew nothing about protecting privacy and those things, even though I'm able to hide most information about me know, information about me in the past can very much lead somebody in a roundabout way to me now. I feel like my privacy is not the best protected in the first place, and with data breaches happening and me being in that vulnerable position I feel even more vulnerable.”

P019’s feelings of vulnerability are profound and extend beyond themselves to those around them with whom they choose to interact in physical spaces as well. “I don't know if I ever feel physically unsafe because I've been through a lot already and I guess I'm at a point where I'm just like if somebody decides to do something what could they do to me? Like there are a million horrible things that could happen to me, but those horrible things could happen to me for no reason, so what could they do to me reasonably? It doesn't make me feel necessarily super physically unsafe. It mostly makes me feel bad for the people who would be around me, like friends who I would have who, like I can't take pictures with ever, ever because that's in my phone. They could have access to any picture in my phone.” *(As a point of clarification, when P019 says “they could have access,” the word “they” refers to malicious people, not companies.)*

P020

P020 was aware of the Facebook breach. She is a white woman between 35-44 years of age, who holds a graduate or professional degree. She has worked in both the for-profit and non-profit sectors. Her approximate annual household income is $200,000 or more. P020's online social media activity is limited to Facebook. Her personal guardianship behaviors are based on limiting access to her posts through Facebook's privacy settings. Her profile is set to "unsearchable," so that people cannot find her account. She has a LinkedIn account, but it is not part of her routine. She found out about the Facebook breach from the news and watched the testimony in Washington before Congress.

P020 has always seen social media as risky. She has assumed from the beginning that information on social media is "not perfectly private." She never trusted Facebook to guard data in the way that maybe the user would like. She also "never really had confidence in [her] own ability to protect [her] information." She thinks that people are generally out for themselves and that scales up to corporations also being out for themselves. After the breach, P020 checked her privacy settings, but made no other changes. She believes that any changes Facebook has made are likely PR motivated.

P020 explained her perception of attackers online "I also think that attackers are getting really, really resourceful, and that in any company it is always possible that someone can breach their data in new and inventive ways." Because of this belief, P020 behaves as though any data she shares might become public at any time. "I try to keep in mind, try to behave in a way that, how do I word this, that I am conscious that anything that I am putting out that it might get picked up by someone else."

P021

P021 was aware of the Facebook breach and affected by the Equifax breach. He is a white man, between 35-44 years of age, who attended college. His approximate annual household income is $35,000 to $49,999. His face-to-face interview regarding the Facebook breach took place on April 18, 2019; he was not interviewed regarding the Equifax breach.

P021’s online social media activity includes Facebook and Twitter daily and Tumblr less frequently. His personal guardianship behaviors include strong passwords and password locked phones. He learned of the Facebook breach from social media posts both posts from friends and from new sites.

P021’s view of risk was not affected by the breach, because he already assumed [his] information's free to read by nearly anyone who wanted to.” He has never considered Facebook a meaningful data guardian. “They are a useful repository and publisher of my data, or at least the stuff I would like to get out there. They're going to get the rest of it along with it.”

After the breach, P021 changed passwords and increase protection for online accounts of which he does value security, such as email accounts. He did not change his protective behaviors on Facebook, because of his assumption that Facebook is inherently insecure. He thinks that any effort’s Facebook is currently making to improve data security are classic examples of closing the barn door after the horses have gone.

When it comes to P021’s own ability to protect his data, he does not see a relationship between his guardianship and external guardians. “My ability to protect my information is about keeping my phone out of people's hands and having decent passwords so casual criminals or ne'er-do-wells can't mess with me. It's a little like home security in the way that I don't think it particularly is possible for me at my level to defend against an actual, professional, or talented, or skilled, or resourced attack. I don't particularly think Facebook is going to, but those are two different things.” He views himself having fairly average self-protection abilities.

P021’s risk assessment has been consistent from his earliest days of internet access. “It's my knowledge of those risks. I don't know how far back we go, but we go all the way back to the BBS era, my knowledge of those risks is what informs my assumption that there are no good data guardians. Not with the kind of data I have. From my very, very first experience with a computer connected to another computer was people going through and reading supposedly private purity teste results and laughing on BBS's. And then later, I won't name names, but someone who was in charge of significant information security in a multi-national, showing how easily publicly accessible databases were, how you could see who had purchased what, and who was what level of whatever, and even trace— We could even sit there on Saturday night and trace financial malfeasance and work out who from what office it had come from, from publicly available data. Those experiences meant I assumed there were no good data guardians.”

P022

P022 was affected by both the Facebook and the Experian breach. She is a white female, between 35-44 years of age, who attended some college. Her approximate annual household income is $100,000 - $149,999. Her face-to-face interview regarding the Facebook breach took place on April 19th, 2019; she was not interviewed regarding the Equifax breach.

P022's online social media activity consists primarily of Facebook and Facebook Messenger every day, Instagram every other day, and Linked In occasionally. Her personal guardianship behaviors include restricting who can see her posts, using passwords and a password manager. Many of the guardianship behaviors are new.

Though she was notified that she was affected by the Facebook breach, the Equifax breach, and at least one other breach within a fairly tight timeframe, the real trigger event for her was an episode of the podcast Reply All that clarified in detail how compromise of less sensitive data could lead to the compromise of more sensitive data. Once she understood these connections, P022 changed her protective behaviors. She got a password manager and began to consider security regularly when online.

Thinking back to before the Facebook breach, P022 says, "what Facebook is did not seem important, what I put on it did not seem important, so how to protect it did not seem important." But now, her view has changed. "It seems more important knowing that people who want our data go to the non-important places to build a profile so they can get to the important places."

P022 does not consider Facebook a data guardian. She equates them with a public space for posting. "I think of them like a bulletin board in a coffee house. It's a place where I can put things. I can control that the people in that coffee house are the ones seeing it, but somebody could wander in, you know?” She does not consider Facebook secure nor does she believe that she is capable of protecting her data online. She sees herself as above average in her ability to enact protective behaviors, but even so does not expect those behaviors to stop motivated offenders. “I think generally it's like having a house. If somebody really wants to step inside, they're gonna come get it.” That risk is “just part of living in the world.”

After the Facebook data breach, P022 actually felt “vindicated,” because it confirmed her belief that Facebook “cannot and do not and would not” protect her data. She sees Facebook as like other companies “I assume 99% of companies are there to make a profit. Facebook is not running Facebook because they think it would be really great if I could keep up with my friends.... If they can sell it, they will. And if they can make a profit off of it, they will.

P022 is somewhat comforted by how wrong Facebook sometimes is about her. “It's only been about two years since we kinda all found out about the secret place in Facebook that shows who they think you are. And you kinda knew they were doing that, but then to see it, you're like, why do they care how close I live to where my parents live? You know what I mean? ... [B]ut it also, so much of it was wrong.... while they're collecting data, they're still making giant assumptions, because I am not a woman of color who lives within five miles of my parents. And you know, there were multiple things that were just completely wrong that I'm like, well, I mean, again, anybody googling me could come up with some ideas, and they actually would probably get a little closer.”

P022’s primary security concern relates to her daughter. She has always been “selective about that” and “Would never post anything that I felt like could be nefarious or whatever.” But she has recently added the step of asking for her daughter’s permission before posting. While her daughter is young, it is important that she have a say. “We had a discussion … I said, ‘Well then, from now on, I need your permission to post about you or post pictures of you or stories about you.’” She is very conscious that other families navigate this issue differently, but for her family for now this works.

P023

P023 was affected by the Facebook breach. He is an African American man, between 25 – 34 years of age, who has attended college. His approximate annual household income is $25,000 to $34,999. His phone interview took place on April 21, 2019.

For P023, a typical day on social media includes Instagram, Twitter, Snapchat, and Patreon. He no longer uses Facebook regularly. He said, "Right now, I'm treating Facebook like a credit card where I keep it open because I have to." He has not deleted his account, though. "I'm not completely closing it out. But yeah. The one good thing about Facebook and Instagram by extension, is that you're able to disable the app."

In terms of personal guardianship, P023 is very selective about both what he posts and who he shares those post with. His one exception to this is political posts: these he makes public. For him, this serves as an incentive to only post political statements he feels strongly enough about to share with the world. He does use a unique password for Facebook, but in general he says that he "go[es] forth in the world when it comes to internet, knowing that [his] stuff has been breached, pretty much."

P023 rejects the idea of risk as an aspect of Facebook use. He says "For me, it's more about exploitation and just how much I'm willing to let people use it to use me for money without getting anything back. Like I said, everything is out in the open there. If you really want to hack something you can do it. If I gave a damn, personally. If I wanted to hack somebody, I could probably figure out how to do it without much effort." Because he sees Facebook as fundamentally exploitative, he is more concerned with "the monetization of people and the fact that it's done so covertly is kind of the more upsetting factor of it."

Nor does P023 have any faith in his own ability to protect his data online. “My confidence in protecting my own information online was already pretty low [before the breach], I guess you might say. That's why my tech savviness and my usage of it is relatively low. But, yeah. I would say ultimately [the breach] did have a negative effect on [my confidence.]” He does believe that he could learn to protect himself more effectively, but at present sees himself as below average in respect to self-protection online.

P023 does not see Facebook as a data guardian. On this topic, he is emphatic. “A data guardian? I have no faith in Facebook as a data guardian whatsoever. When a company amasses billions of dollars in such a short amount of time, the idea of them at all having any kind of perspective towards the best interest of the consumer is laughable, in my opinion.” He points to the complete lack of competitors to Facebook as a contributing factor in this. “So they're essentially a monopoly, and therefore you don't really have any perspective ... you don't have any confidence in their ability to do right by the people.” He also sees a lack of regulations in the tech space as a contributing factor. He does not expect a solution to the regulatory issue to be forthcoming given the advanced age and corruption present in today’s government.

P023 does not feel that Facebook has improved in any way since the breach. In fact he points to recent events, as evidence that they have not solved their underlying problems. “No. I mean, if they're doing anything at all, I think they're just doing something to make themselves look better. Like, recently the New Zealand Park shooting, you know, it was viewed on Facebook a bunch of times, and at first they said "Oh, they only viewed it this small amount of time," and then like, incrementally throughout the day, they were forced to admit how many times it was actually viewed before it got taken down. Now that's not necessarily saying that they weren't trying to block that, because that site is huge on users, so maybe there is a certain... what looks to us like a large chunk, that would filter through without them being able to get it fast enough. That's very possible, but given their tendency to lie about it firsthand makes it seem like they're more concerned about just covering things up instead of actually doing anything."

The New Zealand Park example is a very public example of Facebook failing to moderate a volatile situation, but P023 experiences difficulties with Facebook as a responsible guardian within his own social network. "I'm actually having open communication with a friend right now who's actually going through some issues where she got people who are mass reporting her on stuff because they are psychotic and there's not a real sure-fire way… to combat that." He would like to see Facebook help resolve social and political issues "that Facebook largely helped create."

P024

P024 was aware of the Facebook breach. He is an African American man, between 55-64 years of age, who holds a bachelor's degree. His approximate annual household income is $50,000 - $74,999. His phone interview took place on April 22nd, 2019.

Facebook is the only social media that P024 uses. His son created an Instagram account for him, but he has never posted. He does not consciously take any steps to protect himself online. He does not own a computer; all his Facebook use is through his phone.

P024 heard about the Facebook breach on the news. It didn't affect his feeling of risk online, because he does not feel that he does enough online to be at risk. He has noticed that Facebook has had "a problem with politics in the last couple of years" that he doesn't think they have fixed. He believes that "they've worked to resolve it, but they haven't really come up with anything definite to guarantee our safety."

P024 thinks that Facebook is huge and that that contributes to their difficulties. "I think it's kind of gotten out of their hands, it's so big." He perceives attackers as ubiquitous and difficult for companies to keep ahead of. "Hackers are everywhere, no matter what you try to come up with to stop it, they figure a way around it and then you've got to figure a way to stop that, on and on and on it goes." But he does feel that, because of all the attention, Facebook is making an extra effort to keep data secure right now. He is glad that Facebook is now "taking steps to eliminate certain sites that are deemed dangerous, like terrorist sites and things like that, racist sites."

Overall, Facebook breach didn't affect P024 very much personally. He says, "I'm really a Luddite as far as that stuff goes, I really am. I think I'm stuck in 2002, that's when I gave up technology." He thinks he's below average in his ability to protect himself online, but he isn’t involved enough online for that to matter much to him. He communicates with “really low amount of friends” and has “a small core group of people I talk to every day.” One thing about the breach did have a big effect on P024, however. He remembers “being worried that they were going to go away. "No, no, don't take my Facebook away." He vividly recalls after the breach, “their stock dropped, they lost a bunch of money and I was like, "Uh-oh." A lot of people wanted to boycott Facebook, boycott and I was like, ‘But that's the only thing I use.’” P024 might be a luddite with no computer, but his social interactions on Facebook are an active and valued part of his social support.

Appendix H

IRB Approval

IRB #: PRO-FY2019-311

Title: User Online Routines: Individual Change in the Aftermath of Information Compromise

Creation Date: 1-2-2019

End Date: 1-18-2020

Status: Approved

Principal Investigator: Ruby Booth

Review Board: University of Memphis Full Board

Study History

Submission Type Initial **Review Type** Expedited **Decision** Approved

Submission Type Modification **Review Type** Expedited **Decision** Approved

Key Study Contacts

Member Ruby Booth

Role Principal Investigator

Contact rbooth@memphis.edu

Member Sandra Richardson

Role Co-Principal Investigator

Contact srchrdsn@memphis.edu