

Fall 2015

The design and evaluation of an anonymous, two-way, ethics management reporting system

Jacob A. Young
Louisiana Tech University

Follow this and additional works at: <https://digitalcommons.latech.edu/dissertations>



Part of the [Business Administration, Management, and Operations Commons](#)

Recommended Citation

Young, Jacob A., "" (2015). *Dissertation*. 202.
<https://digitalcommons.latech.edu/dissertations/202>

This Dissertation is brought to you for free and open access by the Graduate School at Louisiana Tech Digital Commons. It has been accepted for inclusion in Doctoral Dissertations by an authorized administrator of Louisiana Tech Digital Commons. For more information, please contact digitalcommons@latech.edu.

**THE DESIGN AND EVALUATION OF AN ANONYMOUS,
TWO-WAY, ETHICS MANAGEMENT
REPORTING SYSTEM**

by

Jacob A. Young, B.S., M.B.A.

A Dissertation Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Business Administration

COLLEGE OF BUSINESS
LOUISIANA TECH UNIVERSITY

November 2015

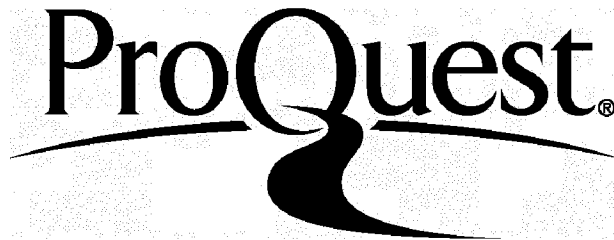
ProQuest Number: 3664534

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest 3664534

Published by ProQuest LLC(2015). Copyright of the Dissertation is held by the Author.

All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code.
Microform Edition © ProQuest LLC.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

LOUISIANA TECH UNIVERSITY

THE GRADUATE SCHOOL

September 25, 2015

Date

We hereby recommend that the dissertation prepared under our supervision by Jacob Alan Young

entitled The Design and Evaluation of an Anonymous, Two-Way, Ethics Management Reporting System

be accepted in partial fulfillment of the requirements for the Degree of Doctor of Business Administration

James F. Courtney
Dr. James F. Courtney, Supervisor of Dissertation Research

T. Selwyn Ellis
Dr. T. Selwyn Ellis, Head of Department
Computer Information Systems

Department

Recommendation concurred in:

Rebecca J. Bennett
Dr. Rebecca J. Bennett, Co-Chair

T. Selwyn Ellis
Dr. T. Selwyn Ellis

M. Clay Posey
Dr. M. Clay Posey

Advisory Committee

Approved: [Signature]
Director of Graduate Studies, Dr. John Francis

[Signature]
Dean of the College, Dr. Christopher Martin

Approved: [Signature]
Dean of the Graduate School, Dr. Sheryl Shoemaker

[Signature]
Dean of the Graduate School, Dr. Sheryl Shoemaker

ABSTRACT

Despite a recognized need for whistleblowing systems in academic research, little to no attention has been given to the necessary requirements for and specific design of effective whistleblowing systems. In order to increase the rate of reporting, it is critical for reporting systems to be designed with the intent to reduce employee fears and inhibitions by reducing the potential for retaliation. Therefore, the goal of this three-essay dissertation was to enhance a firm's ability to solicit and investigate concerns by proposing and evaluating a system aimed at fostering anonymous, two-way communication between employees and investigators of wrongdoing.

In essay one, design science (Hevner et al., 2004; March & Smith, 1995; Walls, Widmeyer, & El Sawy, 1992, 2004) was employed in order to theorize and justify the design of an anonymous reporting system artifact. In doing so, existing reporting systems were examined and modern technologies were incorporated into a proposed design of an anonymous, two-way ethics management reporting system.

Essay two reviewed existing theories in the extant whistleblowing literature and relied upon communication research, both inter-personal and computer-mediated, to address the limitations of prior theory regarding reduced perceptions of credibility for anonymous whistleblowers. The experiment tasked subjects with evaluating simulated two-way communication between an investigator and an employee attempting to blow the whistle on financial wrongdoing. The results provide strong evidence that two-way


communication can reduce the credibility gap between perceptions of anonymous and identified whistleblowers.

Lastly, essay three assessed the system design proposed in essay one from the perspective of the organizational insider. The proposed system was also compared to other channels available to report wrongdoing, such as the use of open door policies and telephone hotlines. Two simultaneous online experiments tested user perceptions of anonymity protections provided by each channel, as well as the specific whistleblower-oriented design features proposed in the design. This essay provides evidence that online reporting systems are perceived to provide significantly higher anonymity protections than phone hotlines and open door policies, while select features of the proposed system impact user perceptions of anonymity.

APPROVAL FOR SCHOLARLY DISSEMINATION

The author grants to the Prescott Memorial Library of Louisiana Tech University the right to reproduce, by appropriate methods, upon request, any or all portions of this Dissertation. It is understood that "proper request" consists of the agreement, on the part of the requesting party, that said reproduction is for his personal use and that subsequent reproduction will not occur without written approval of the author of this Dissertation. Further, any portions of the Dissertation used in books, papers, and other works must be appropriately referenced to this Dissertation.

Finally, the author of this Dissertation reserves the right to publish freely, in the literature, at any time, any or all portions of this Dissertation.

Author 
Date 10/28/15

DEDICATION

To my parents, Michael and Dana Young,
who have always supported me in all of my pursuits.

To my sister and brother, Jessica Miller and Joshua Young,
who have always been my biggest fans.

To my uncle, Richard Henry, who has never hesitated to provide love,
encouragement, and a delicious ribeye.

To my grandparents, who always encouraged me to do what is right,
no matter the consequences.

TABLE OF CONTENTS

ABSTRACT.....	iii
DEDICATION.....	vi
LIST OF TABLES.....	xiii
LIST OF FIGURES	xvi
ACKNOWLEDGEMENTS.....	xviii
CHAPTER ONE – INTRODUCTION.....	1
Literature Review.....	4
Ethics Management Reporting.....	5
Employee Silence.....	8
Retaliation	10
Anonymity	13
Research Questions.....	17
Research Studies	17
CHAPTER TWO – THE DESIGN OF AN ANONYMOUS, TWO-WAY, ETHICS MANAGEMENT REPORTING SYSTEM	19
Introduction.....	19
Literature Review.....	21
Design Science.....	22
Activities and outputs	22
Research guidelines	24

Design theory	26
Ethics Management.....	28
Internal reporting	30
External reporting	30
Internal whistleblowing	31
External whistleblowing	31
Two-Way Communication.....	32
Anonymity, Unlinkability, and Undetectability! Oh, my!	34
Onion Routing.....	36
Existing Reporting Channels	37
Open door policy.....	37
Postal mail.....	38
Telephone.....	38
Fax.....	39
Web forms.....	39
Email	40
Existing Reporting Systems	41
Threat Analysis	43
Organizational Insiders	43
Organizations	43
Investigators	44
Attackers	45
Research Questions.....	47
Design Principles	48

Free Software	48
Kerckhoffs' Principles for Cryptography	49
Proposed System Design.....	50
System Use Case.....	53
System Features	55
Data Encryption	57
Symmetric algorithms.....	57
Asymmetric encryption.....	57
Forward secrecy	58
Tor Anonymity Network.....	58
Common attacks.....	62
Tor Browser Bundle.....	62
Tor Hidden Services	62
The Amnesic Incognito Live System (Tails).....	67
Metadata Anonymization.....	67
User Authentication	68
Multifactor authentication.....	70
Passwords.....	71
Passphrases	72
Authenticating whistleblowers.....	73
Authenticating investigators	73
Two-Way Anonymous Messaging	73
Investigation Status.....	74
Text-Analysis.....	74

Additional Considerations	75
Best Practices for Investigators.....	75
Reporting Metrics	75
Contributions.....	76
Conclusion	77
CHAPTER THREE – THE IMPACT OF ANONYMOUS, TWO-WAY COMMUNICATION ON PERCEIVED WHISTLEBLOWER CREDIBILITY	78
Introduction.....	78
Literature Review.....	79
Models of Communication	79
Media Richness Theory	82
Communication in Whistleblowing	84
Role of anonymity.....	85
Hypotheses Development	86
Methodology	89
Participants.....	89
Experimental Design.....	89
Procedure	90
Manipulation Checks	97
Results.....	98
Sample Demographics	98
Hypotheses Tests	101
Discussion.....	107
Practical Implications.....	108

Research Implications.....	108
Conclusion.....	109
CHAPTER FOUR – PERCEPTIONS OF ANONYMITY PROTECTIONS PROVIDED BY ETHICS MANAGEMENT REPORTING CHANNELS	111
Introduction.....	111
Theoretical Background.....	111
Anonymity vs. Confidentiality	112
Limitations of Existing Reporting Channels.....	112
Open door policy.....	112
Phone hotline	113
Online reporting system.....	116
Proposed System Features	117
Data encryption.....	117
Tor Web Browser.....	118
Meta-data scrubbing.....	119
Development method	120
Authentication.....	121
Research Questions.....	122
Hypotheses Development	122
Reporting Channels.....	123
System Features	124
Methodology	125
Manipulation Checks	130
Measures	130
Results.....	133

Sample Demographics	133
Hypothesis Tests	135
Discussion	145
Perceptions of Reporting Channels.....	145
Perceptions of Online Reporting Systems	145
Implications for Practice	145
Contributions to the Literature.....	146
Suggestions for Future Research	146
Limitations	146
Conclusion	146
CHAPTER FIVE – CONCLUSION.....	148
Implications for Practice	149
Academic Contributions	150
Future Research	151
APPENDIX A – HUMAN USE APPROVAL LETTER (HUC 1296)	153
APPENDIX B – HUMAN USE APPROVAL LETTER (HUC 1323)	155
REFERENCES	157

LIST OF TABLES

Table 1.1	Retaliation Against Whistleblowers (Ethics Resource Center, 2013)	12
Table 2.1	Activities of Design Science Research (March & Smith, 1995)	23
Table 2.2	Outputs of Design Science Research (March & Smith, 1995)	24
Table 2.3	Design Science Research Guidelines (Hevner et al., 2004).....	25
Table 2.4	Information System Design Theory (Walls et al., 1992, 2004)	26
Table 2.5	Design Theory for Anonymous, Two-Way Ethics Management Systems	28
Table 2.6	Typology of Ethics Management Reporting (MacNab et al., 2007).....	29
Table 2.7	Definitions Related to Anonymity (Pfitzmann & Hansen, 2010).....	35
Table 2.8	Existing Reporting Channels	41
Table 2.9	Existing Reporting Systems.....	42
Table 2.10	Capabilities, Methods and Other Means of the Attacker (The Amnesic Incognito Live System, 2015).....	47
Table 2.11	Essential Freedoms of Free Software (Free Software Foundation, 2015)	48
Table 2.12	Kerckhoffs' Principles for Cryptography (Kahn, 1996, p. 235)	50
Table 2.13	Proposed Features of Ethics Management Reporting Systems.....	56
Table 2.14	Advantages and Disadvantages of Authentication Factors.....	70
Table 3.1	Daft & Lengel's (1984) Hierarchy of Media Richness	83
Table 3.2	Experimental Treatments	93
Table 3.3	Simulated Communication from Whistleblower	94
Table 3.4	ANOVA Results for Manipulation Checks	97

Table 3.5	Sample Gender.....	98
Table 3.6	Sample Age.....	98
Table 3.7	Sample Education Level.....	99
Table 3.8	Organizational Tenure.....	99
Table 3.9	Type of Organization.....	100
Table 3.10	Industries Represented.....	100
Table 3.11	Descriptive Statistics for Treatment Groups.....	101
Table 3.12	ANOVA Results for Main Effects.....	102
Table 3.13	Tests of Homogeneity of Variance.....	102
Table 3.14	Planned Comparisons Contrast Coefficients.....	103
Table 3.15	ANOVA Results for Planned Comparisons.....	104
Table 3.16	Summary of Results.....	107
Table 4.1	Description of the Open Door Policy.....	127
Table 4.2	Description of the Phone Hotline.....	127
Table 4.3	Manipulations Employed in the Online Reporting System Description.....	128
Table 4.4	Scenarios.....	129
Table 4.5	System Feature Manipulation Checks.....	130
Table 4.6	Model Fit for the Confidence in Reporting Channel Anonymity CFA.....	131
Table 4.7	Online Reporting System Anonymity.....	132
Table 4.8	Sample Gender.....	133
Table 4.9	Sample Age.....	133
Table 4.10	Sample Education Level.....	134
Table 4.11	Organizational Tenure.....	134
Table 4.12	Type of Organization.....	134

Table 4.13	Industry	135
Table 4.14	Paired Samples Test of Reporting Channel Perceptions.....	136
Table 4.15	Tests of Between-Subjects Effects for Proposed System Features.....	137
Table 4.16	Summary of Results.....	144

LIST OF FIGURES

Figure 2.1	Information Systems Research Framework (Hevner et al., 2004).....	25
Figure 2.2	Relationships Among ISDT Components (Walls et al., 1992, 2004).....	27
Figure 2.3	Addition of Barnlund's (1970) Feedback to Berlo's (1960) SMRC Model	33
Figure 2.4	Barnlund's (1970) Transactional Model of Communication	33
Figure 2.5	Onion Routing (Goldschlag, Reed, & Syverson, 1996).....	37
Figure 2.6	Overview of the Proposed System Design.....	52
Figure 2.7	Use Case for the Proposed System	54
Figure 2.8	Onion Routing.....	59
Figure 2.9	How Tor Works: 1 (The Tor Project, 2015b)	60
Figure 2.10	How Tor Works: 2 (The Tor Project, 2015b)	61
Figure 2.11	How Tor Works: 3 (The Tor Project, 2015b)	61
Figure 2.12	Tor Hidden Services: 1 (The Tor Project, 2015a).....	64
Figure 2.13	Tor Hidden Services: 2 (The Tor Project, 2015a).....	64
Figure 2.14	Tor Hidden Services: 3 (The Tor Project, 2015a).....	65
Figure 2.15	Tor Hidden Services: 4 (The Tor Project, 2015a).....	65
Figure 2.16	Tor Hidden Services: 5 (The Tor Project, 2015a).....	66
Figure 2.17	Tor Hidden Services: 6 (The Tor Project, 2015a).....	66
Figure 2.18	Comic courtesy of XKCD (https://xkcd.com/936/)	72
Figure 3.1	Shannon's (1948) Model of the Communication Process	80
Figure 3.2	Berlo's (1960) SMCR Model of Communication	80

Figure 3.3	Addition of Barnlund's (1970) Feedback to Berlo's (1960) SMRC Model	81
Figure 3.4	Barnlund's (1970) Transactional Model of Communication	82
Figure 3.5	Communication Effectiveness Continuum for Common Mediums.....	84
Figure 3.6	Background Information.....	90
Figure 3.7	Financial Reports for Vitrum Technologies, Inc.	91
Figure 3.8	Organizational Chart for Vitrum Technologies, Inc.	92
Figure 3.9	Screenshot of Simulated Communication.....	95
Figure 3.10	Resource Allocation Measure	96
Figure 4.1	Number of Payphones in the United States (U.S. Federal Communications Commission, 2014)	115

ACKNOWLEDGEMENTS

This dissertation would not have been possible without the tremendous support provided by my committee. I had the good fortune of receiving guidance from two distinguished co-chairs in Dr. Jim Courtney and Dr. Rebecca Bennett, who provided continuous encouragement and direction throughout the course of conducting this research. I must give an extra special thanks to Dr. Selwyn Ellis for his unwavering support and belief in me while I pursued my doctoral studies. I must also thank Dr. Clay Posey, whose insightful feedback enhanced my dissertation immensely. I would like to thank all of the faculty members, especially Dr. David Thomson, Dr. John Hall, Dr. Marck Beggs, Dr. Frank Smith, and Dr. Tom Roberts, who imparted their knowledge and wisdom to me throughout my academic career. I would like to thank my fellow doctoral students—those who have moved on, those who remain, and those just beginning—for their support, feedback, and friendship. Lastly, I must thank all of my family and friends for their love and understanding, especially over the past three years. I will never be able to fully express how much it has meant to me.

CHAPTER ONE

INTRODUCTION

“Man is least himself when he talks in his own person.

Give him a mask, and he will tell you the truth.”

– Oscar Wilde, *The Critic as Artist* (1891)

The need for greater organizational self-governance has received increased attention in recent years due to a number of major corporate scandals in the United States, such as those which resulted in the demise of Enron, Worldcom and Tyco. While high profile cases of misconduct are well known, a wide variety of undesirable business practices and employee behaviors also plague the business world. It is estimated that over one third of employees have observed misconduct within their organization (Rothschild & Miethe, 1999), yet only one quarter of those who observe wrongdoing will report it (Near, Rehg, Van Scotter, & Miceli, 2004). Despite the low incidence of reporting, the fact that employees were responsible for uncovering 17% of the alleged corporate frauds involving U.S. companies with more than 750 million U.S. dollars in assets between 1996 and 2004 shows that employee reporting can be highly effective at detecting wrongdoing within organizations (Dyck, Morse, & Zingales, 2010). Thus, it is clear that those within the organization are well suited to serve as a first line of defense for

organizations in detecting and reporting wrongdoing in the form of behavior termed *whistleblowing* (Ayers & Kaplan, 2005; Miceli, Near, & Dworkin, 2008b; Miceli & Near, 2005). Therefore, organizations should ensure that reports of wrongdoing are accurate and credible, and encourage the remaining three quarters of employees who observed wrongdoing but failed to report the issue, to come forward and report.

While socially desirable in its own right, firms also have self-serving strategic, financial and legal motivations for encouraging whistleblowing in order to prevent wrongdoing within their organizations (Bamberger, 2006; Callahan & Dworkin, 1992; Kaptein, 2010; Karpoff, Lee, & Martin, 2008; Schnatterly, 2003). The U.S. has passed a number of laws with provisions, such as those contained within the Sarbanes-Oxley Act of 2002 and the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which provide increased internal and external regulation and oversight in order to address corporate misconduct. Both pieces of legislation, among others, expand the legal requirements for anonymous reporting channels, provide greater employee protection against retaliation and increase potential monetary rewards for effective cases of whistleblowing (Kohn, 2011). For example, the U.S. Securities and Exchange Commission (SEC) has awarded as much as \$14 and \$30 million under the Dodd-Frank to individual whistleblowers for their role in uncovering wrongdoing (U.S. Securities and Exchange Commission, 2013, 2014). However, the first payment to a victim of retaliation was awarded to Candace King Weir in 2015, as a result of her employer's retaliatory actions after discovering she had reported misconduct to the SEC (U.S. Securities and Exchange Commission, 2015). As of April 28, 2015, the SEC had awarded payments to 17 whistleblowers totaling over \$50 million. Despite these cases, the legislation has been

criticized for not outlining specific requirements to ensure compliance and essentially relies on the organization's "good faith," which might allow management to effectively skirt the true intent of the law and leave employees vulnerable to retaliation (Devine & Maassarani, 2011, pp. 84–85; Kohn, 2011, pp. 119–122).

Although whistleblowing has received considerable attention in the media and academic literature over the past 30 years (Bjørkelo, Bye, & Bj, 2014; Mesmer-Magnus & Viswesvaran, 2005; Miceli & Near, 2005; Near & Miceli, 1996; Olsen, 2014; Vandekerckhove, Uys, Rehg, & Brown, 2014), there has been limited research focused on a critically overlooked component of modern whistleblowing; that is, the reporting system itself. Despite a recognized need for such systems in academic research (Elias, 2008; Hassink, Vries, & Bollen, 2007; Lowry, Moody, Galletta, & Vance, 2013; MacNab & Worthley, 2007; C. Park & Keil, 2009; Silowash et al., 2012), little to no attention has been given to the necessary requirements for and specific design of effective whistleblowing systems. It is critical for reporting system design to (1) reduce employee fears and inhibitions in order to increase the rate of reporting, while also (2) assisting investigators in determining the credibility and accuracy of reports. Therefore, the primary goal of this research is to enhance a firm's ability to solicit and investigate internal concerns by proposing a system design aimed at fostering anonymous, two-way communication between employees and investigators. Those who are responsible for investigating reports, such as auditors and compliance officers, will determine the efficacy of two-way communication for improving the assessment of anonymous report credibility. Further, organizational insiders' intention to adopt and use the proposed system design will be compared to that of existing reporting channels already in practice.

Literature Review

Individuals use *voice* in order to provide others with suggestions as well as concerns (Van Dyne, Ang, & Botero, 2003). Liang et al. (2012) proposed two specific types of voice: *prohibitive voice* and *promotive voice*. Prohibitive voice consists of “expressions of concern about work practices, incidents, or employee behavior that are harmful to their organization,” while promotive voice is the “expression of new ideas or suggestions for improving the overall functioning of their work unit or organization” (Liang et al., 2012, p. 75). Because whistleblowing is “when current or former employees disclose illegal, immoral, or illegitimate organizational activity to parties they believe may be able to stop it” (Miceli, Near, & Dworkin, 2008a) and is effective only when “the questionable or wrongful practice (or omission) is terminated at least partly because of whistleblowing and within a reasonable time frame” (Near & Miceli, 1995), employees wishing to blow the whistle on misconduct within their organization would do so using a prohibitive voice (Miceli & Near, 2013).

Organizations can also benefit from improved communication within the organization when employees use a promotive voice to provide other types of constructive feedback, whether they be opinions, concerns or ideas (Knoll & Dick, 2012; MacNab et al., 2007; Park & Keil, 2009; Smith & Keil, 2003; Tangirala & Ramanujam, 2008; Van Dyne et al., 2003). Since simply *speaking up* (Ashford, Rothbard, Piderit, & Dutton, 1998; Miceli & Near, 1992; Withey & Cooper, 1989) using a promotive voice within the organization would not always meet the definition of whistleblowing, a more inclusive term, *ethics management reporting*, has been proposed in order to more accurately differentiate the various types of disclosure (MacNab et al., 2007).

Ethics Management Reporting

Whistleblowing has been classified as a pro-social organizational behavior (Miceli & Near, 1992) and internal reporting has been viewed as a protection-motivated behavior (Posey, Roberts, Lowry, Bennett, & Courtney, 2013), both of which employees can utilize to report instances of wrongdoing and misconduct observed within the organization. While the term *whistleblowing* is often widely applied to any disclosure of wrongdoing, it is important to distinguish the key differences among the four types of ethics management reporting: (1) *internal reporting*, (2) *external reporting*, (3) *internal whistleblowing*, and (4) *external whistleblowing* (MacNab et al., 2007). Regardless of whether the disclosure is made internally or externally, the primary distinction between reporting and whistleblowing is that reporting is conducted through organizationally authorized channels, whereas whistleblowing occurs when an employee does not follow the organization's official reporting policy. Wrongdoing and misconduct uncovered through external whistleblowing, as opposed to internal reporting, can result in higher legal costs, more severe legal sentencing, decreased sales, and negative publicity (Barnett, Cochran, & Taylor, 1993). Therefore, it is critically important for organizations to solicit feedback from employees in order to obtain a wider view of questionable behavior within the organization and address concerns before they result in significant damage.

Internal reporting occurs when an employee utilizes an organization's officially authorized channel to report wrongdoing to an empowered entity within the organization itself. Authorized channels are communicated to employees through an organization's policies, procedures and/or training. An example of internal reporting would include the reporting of misconduct using an authorized internal reporting channel, such as open door

policies, an ethics ombudsman or telephone hotline (Kaptein, 2002). While establishing an internal reporting channel for employees is only explicitly required for publicly traded firms in the U.S., it would also be wise for private firms to voluntarily implement internal reporting policies, procedures and systems.

External reporting is also authorized by the organization, but allows for reports to be received by an outside entity, such as independent auditors or third-party compliance firms. Although reporting to an independent entity outside of the organization may be perceived as more effective by employees and can allow for increased employee anonymity and confidentiality, external reporting can also result in a decrease in investigation efficiency due to an investigator's reduced knowledge of the inner workings of the organization (Kaptein, 2002).

Internal whistleblowing is classified as reporting conducted within the organization, but via unauthorized channels. An example of internal whistleblowing would be when an employee does not follow an organization's policy of first reporting any concerns to his or her direct supervisor and instead elects to inform higher management. While an organization can still maintain control over a case of internal whistleblowing, the rate of retaliation may increase since the employee elected to not follow the established reporting procedure.

External whistleblowing occurs when an employee elects to disclose misconduct to an outside party that the organization has not endorsed, such as the media, a government agency, a non-governmental organization, or a professional organization (Kaptein, 2010). From an organization's perspective external whistleblowing can be a manager's nightmare as it is viewed as a data breach that is likely to lead to negative

publicity, regulatory investigations, and legal liability (Barnett et al., 1993). Rothschild & Miethe (1999) found that employees are more likely to resort to external whistleblowing “once they come to believe that internal channels are closed to them, that the organization is not moral, and that senior management is inert or complicit in the wrongdoing.” Consistent with these findings, Sims & Keenan (1998) concluded that lack of supervisor support, informal policies, gender, and ideal values are significantly related to external whistleblowing. The Ethics Resource Center (2013) reported a number of similar findings. For example, 45% of external whistleblowers did not trust anyone within the organization and 40% experienced retaliation after first reporting internally. At the same time, a combined 65% reported that the organization either failed to act on the internal report or that the whistleblower decided to report externally after becoming dissatisfied with the outcome. Therefore, the culture of the organization is critical to reducing the incidence of external whistleblowing.

While some ethicists have argued that directly confronting the alleged wrongdoer(s) is the only moral option initially available to an employee who wishes to report misconduct (Bowie, 1982; DeGeorge, 1986; Velasquez, 2005), others have reasoned that electing to use other channels is acceptable under certain conditions, such as if the employee perceives a threat of retaliation or when first attempts to solve the issue prove to be unsuccessful (Kaptein, 2002; Larmer, 1992; Miceli & Near, 1992). Therefore, while the ordering of each type of ethics management reporting is consistent with a logical progression from most to least desirable (i.e., from authorized to unauthorized and internal to external), some employees may elect to skip one or more of the channels due to a fear of retaliation and/or a culture of organizational silence, both of

which will be discussed in the following sections. For the sake of simplicity, unless a particular type of reporting or whistleblowing is specified, any future use of the terms “whistleblowing” and “whistleblower” in the remainder of this proposal are to be interpreted in a general sense and refer to the act of disclosing wrongdoing and those who elect to come forward, respectively.

Employee Silence

When looking at the four types of ethics management reporting from an organization’s perspective, it is clear that internal reporting would be the preferred option (Near & Miceli, 1996; Near, 1989). This is also true for employees whose organizations are perceived to be supportive of employee voice in that they are more likely to raise their concerns internally (Rothschild & Miethe, 1999). Unfortunately, many organizations may suffer from a culture of *employee silence*, which has the potential to severely limit the incidence of internal reporting and consequently increase the likelihood of external whistleblowing (Barnett et al., 1993; Jos, Tompkins, & Hays, 1989; Miceli & Near, 1985, 1992; Near & Jensen, 1983; Near & Miceli, 1986, 1996). Morrison & Milliken (2000) originally proposed *organizational silence* in an effort to investigate the higher-level organizational, rather than personal, factors which might influence the reporting climate of an organization. Organizational silence refers to “a state in which employees refrain from calling attention to issues at work such as illegal or immoral practices or developments that violate personal, moral, or legal standards” (Knoll & van Dick, 2013). Knoll & Dick (2012) extended the earlier work on employee silence into a multidimensional construct composed of four types: 1) *pro-social*, 2) *opportunistic*, 3) *acquiescent*, and 4) *quiescent*.

Van Dyne et al. (2003) added pro-social motives to Pinder & Harlos' (2001) work on employee silence to develop the concept of pro-social silence, which is defined as “withholding work-related ideas, information, or opinions with the goal of benefiting other people or the organization—based on altruism or cooperative motives” (Van Dyne et al., 2003, p. 1368). An example of pro-social silence would be the protection of proprietary information such as an organization’s future business strategies or the secret formula for a highly successful soft drink. Knoll & Dick (2012, p. 351) suggest that individuals may engage in pro-social silence due to “a general altruistic personality, a high motive for affiliation, but also interest in maintaining social capital (Adler & Kwon, 2002) and protecting social identity (Ashforth & Mael, 1989)” within the organization. Knoll & Dick (2012) point out that while withholding information through pro-social silence for the benefit of the organization is valuable, a self-interested type of employee silence, referred to as opportunistic silence, can also negatively impact the organization.

Opportunistic silence is defined as “strategically withholding work-related ideas, information, or opinions with the goal of achieving an advantage for oneself while accepting harm of others” (Knoll & van Dick, 2013, p. 351). An employee might engage in this type of silence in an attempt to gain or maintain control over a particular aspect of the organization.

While ethics management reporting would not be expected to have a significant impact on the first two types of silence, effective ethics management reporting provides an avenue for employees to overcome an organizational environment of suffering from the following two types, acquiescent and quiescent silence.

Acquiescent silence occurs when employees eventually stop reporting wrongdoing after experiencing multiple failed attempts to enact change or when they feel that their opinion is not valued by the organization (Morrison & Milliken, 2000). This type of employee silence was proposed by Pinder & Harlos (2001) and occurs when employees are so demotivated that they passively withhold relevant ideas out of submission and resignation (Knoll & van Dick, 2013). Management must be aware of this possibility and ensure that employees perceive the internal reporting program as an effective tool for resolving concerns or else the organization will experience a decrease in the number of reports, which prevents the organization from benefiting from internal disclosures.

Finally, quiescent silence was introduced by Pinder & Harlos (2001) and refers to “the active withholding of relevant information in order to protect oneself, based on the fear that the consequences of speaking up could be personally unpleasant” (Knoll & Dick, 2012, p. 351). This type of silence is consistent with Near & Miceli's (1995) theory that the decision to not report wrongdoing is likely driven by the fact that most employees are more dependent upon the organization as a source of livelihood than the organization depends upon them as employees. Due to this imbalance, employees who would otherwise report misconduct may elect to remain silent in order to avoid any possibility of retaliation from the organization or individuals involved.

Retaliation

With the discussion of employee silence in mind, it is easy to understand how employees must feel that raising concerns will be effective and without unreasonable personal consequences before deciding to blow the whistle (Ashford et al., 1998; Miceli

& Near, 1992; Morrison & Milliken, 2000; Withey & Cooper, 1989). Unfortunately, retaliation against those who speak up is quite common (Rothschild & Miethe, 1999) and is “most likely and most severe when the observed wrongdoing is most systemic and most central to the operation of the agency” (Rothschild & Miethe, 1999, p. 125). Retaliation can be levied in many forms, such as: nullification, isolation, defamation, expulsion, ostracism, demotion, or termination (Barnett et al., 1993; Dworkin & Baucus, 1998; Kaptein, 2010). Rothschild & Miethe (1999) report that approximately two thirds of the whistleblowers in their study had experienced the following forms of retaliation: 69% lost their job or were forced to retire; 64% received negative job performance evaluations; 68% had work more closely monitored by supervisors; 69% were criticized or avoided by coworkers; and 64% were blacklisted from getting another job in their field. The authors further note that the rate of retaliation due to whistleblowing was approximately 10 to 15% higher for those who elected to report their concerns externally. However, these effects are not limited to within the organization. Whistleblowers often find themselves cut off from friends, family and/or outside colleagues. John Brown, as he is referred to under a pseudonym by Alford (2001), refused to lie to the FBI to protect his boss and described his experiences this way:

The Engineers Association, they just wished me luck, said they admired someone who stood up for their beliefs. Take that to the bank. They wouldn't even help me find a new job. Nobody understands. Lots of people say they admire my spunk, but nobody has any idea of the consequences. No one wants to know. (Alford, 2001, p. 2)

Further, whistleblowers report alarmingly high incidences of emotional, mental and physical stress, such as: severe depression or anxiety (84%), feelings of isolation or powerlessness (84%), distrust of others (78%), declining physical health (69%), severe financial decline (66%), and problems with family relations (53%) (Rothschild & Miethe,

1999). Similar findings have been reported by the Ethics Resource Center (2013), which has been reproduced in Table 1.1.

Table 1.1 – Retaliation Against Whistleblowers (Ethics Resource Center, 2013)

Type of Retaliation	2011	2013
Supervisor intentionally ignored or began treating differently		69%
Other employees intentionally ignored or began treating differently	62%	59%
Supervisor or management excluded from decisions and work activity	64%	54%
Verbally abused by supervisor or someone else in management	62%	49%
Not given promotions or raises	55%	47%
Verbally abused by other employees	51%	43%
Almost lost job	56%	38%
Hours or pay were cut	46%	29%
Relocated or reassigned	44%	28%
Demoted	32%	21%
Harassed at home	29%	18%
Experienced physical harm to person or property	31%	16%
Experienced online harassment	31%	15%

Due to the severe anguish felt by a whistleblower that has experienced retaliation, he or she may ultimately regret the decision to blow the whistle. These experiences and resulting regret may lead employees to avoid whistleblowing in the future by remaining acquiescent and/or quiescent silent due to the effect retaliation has had on their trust in others, both inside and outside of the organization. This reality is commonly heard in the statements of whistleblowers upon reflection, such as:

I keep my mouth shut these days. I'm a different person now. I don't know. In hindsight I wouldn't have said anything ... I wouldn't have because it caused so much stress and it wasn't worth it really, like emotionally. It was really tough going to work for so long... you're just, you know, dreading going to work. (Jackson et al., 2010, p. 2198)

If I had to do it over again, I wouldn't blow the whistle for a million dollars. It ruined my life. My neighbor kept talking about all of these stories he'd read about "the little man who stood up against the big corporation and won." Well, I stood up against the big corporation and I lost. I didn't just lose my job. I lost my house, and then I lost my family. I don't even see my kids anymore. My ex-father-in-law said if I'd been a real whistleblower I'd have been on *60 Minutes*. (Alford, 2001, p. 1)

Retaliation against whistleblowers may occur for a variety of reasons. For example, the organization may rely upon the individual responsible for the wrongdoing, management may see no other alternative than to continue the wrongdoing or may simply believe that suppressing the disclosure will reduce or eliminate additional consequences (Near & Miceli, 1995). While retaliation has been shown to reduce the incidence of internal reporting and internal whistleblowing, actual or threatened retaliation is not an effective approach to silencing employees or suppressing revelations of organizational misconduct as the mere perception of a retaliatory climate only compounds the problem for the organization due to a higher likelihood of external whistleblowing (Barnett et al., 1993; Jos et al., 1989; Miceli & Near, 1985, 1992; Near & Jensen, 1983; Near & Miceli, 1986, 1996). Further, retaliation is more likely to result in far more damaging and public outcomes for the organization, such as negative publicity, regulatory investigations, and legal liability (Barnett et al., 1993). Therefore, rather than treat those who report wrongdoing as adversaries, management would be better served to view such disclosures as an opportunity to improve the organization (Barnett et al., 1993).

Anonymity

While the solicitation of feedback of unethical or illegal behavior from employees has the potential to result in corrective action, fostering an organizational culture that is open to the voluntary reporting of wrongdoing or misconduct is challenging due to the

sensitive nature of reporting and the potential threat of retaliation. Therefore, organizations should focus on instilling measures that provide a safe environment and culture for reporting. Ensuring anonymity is one avenue for organizations to develop safer climates for whistleblowing. *Anonymity* is generally defined by the Merriam-Webster dictionary as “the quality or state of being unknown to most people.” Due to the threat of retaliation, whistleblowers must have assurances that their identity will not be revealed. The need to protect employees from retaliation is evident in the fact that the Sarbanes-Oxley Act of 2002 requires publicly traded companies to provide anonymous communication channels for employees to report wrongdoing. Anonymity measures incorporated into policies, procedures and systems for the reporting of wrongdoing can address these concerns. This is due to the fact that employees perceive reporting via anonymous channels as less likely to result in employment loss, reputation loss, or harassment (Ayers & Kaplan, 2005; Kaplan & Schultz, 2006, 2007; Near & Miceli, 1995, 1996) and has been shown to result in a more open and thorough exchange of ideas in computer-mediated communication (Jessup & Tansik, 1991). Therefore, anonymity measures must be in place to provide a safe channel for reporting prior to blowing the whistle and can protect the employee from retaliation after submitting a report.

While anonymity has been championed as a protection measure for whistleblowers for decades, truly achieving such anonymity is far more difficult and can significantly complicate the investigation process. Firstly, a system provides *sender-anonymity* if, and only if, the system prevents the receiver, or any other party, from identifying the sender (Sherwood, Bhattacharjee, & Srinivasan, 2005). This is extremely difficult to achieve in most cases since a simple process of elimination can oftentimes

identify the possible senders or recipients for a given message. Therefore, the degree of sender-anonymity provided by any system is dependent upon the size of the set of people who could have sent/received a particular message (Sherwood et al., 2005).

Secondly, regardless of a system's ability to provide sender-anonymity, in some cases it might be impossible to completely disassociate the whistleblower from the content of his or her report and/or the context of the situation being reported (Kaptein, 2002). For example, a salesman who reports the misconduct of a colleague that occurred while both were the only two employees away from the office on a business trip would not provide any reasonable level of anonymity protection. Therefore, it is important for organizations to consider authorizing external reporting to independent parties. Proper handling of external reporting provides greater anonymity protection for the employee in the event that he or she unintentionally reveals their identity. For example, the independent party can remove any potentially identifying information prior to informing the organization of the alleged wrongdoing.

Thirdly, the nature of anonymous reporting has resulted in organizations adopting reporting systems that prevent investigators from further communication with the whistleblower beyond the initial report (Ayers & Kaplan, 2005; Kaptein, 2002; Miceli et al., 2008b, p. 158). While one might consider a system that prevents an investigator from contacting the employee as having effective anonymity measures, the inability to obtain additional information from the initial report can reduce the effectiveness of the investigation. Investigators might need to request additional information from employees in order to clarify the alleged wrongdoing, obtain more evidence, or simply improve the efficiency of the investigation. Further, without the ability to contact the author of an

anonymous report, investigators cannot provide status updates during the investigation or discuss how a particular case was resolved, which is critical to demonstrating the effectiveness of reporting wrongdoing. If employees perceive that their willingness to report wrongdoing failed to yield effective results, they may be less likely to blow the whistle in the future.

Lastly, researchers have suggested that the use of anonymous reporting channels might actually undermine the investigation process. It has been theorized that investigators' might perceive anonymous reports as being less credible than those from identified individuals (Kaplan & Schultz, 2006, 2007; Near & Miceli, 1995, 1996), while potential whistleblowers' also perceive the use of anonymous channels as less effective at reaching their desired outcome (Dyck et al., 2010; Miceli et al., 2008b, p. 158). Further, Dyck et al. (2010) found that the rate of reporting wrongdoing actually declined from 18% to 13% following the mandatory implementation of anonymous channels required by the *Sarbanes-Oxley Act of 2002*. Therefore, despite the need for anonymity measures to protect whistleblowers, the use of anonymity reduces the likelihood of reporting and complicates the investigation process, which ultimately reduces the likelihood of correcting the wrongdoing. While these findings are discouraging, this dissertation proposes several remedies for closing the credibility gap between non-anonymous and anonymous reporting channels through the use of recent advancements in technology.

Management practices are also critical to the success of internal reporting programs and the failure to provide a safe environment for raising concerns “foolishly invites catastrophe” (Callahan, Dworkin, Fort, & Schipani, 2002, p. 195) and will ultimately lead to employee silence and less desirable forms of ethics management

reporting, such as external whistleblowing (Callahan et al., 2002; Jos et al., 1989; Miceli & Near, 1985; Near & Jensen, 1983; Near & Miceli, 1986). Employee perceptions of which behaviors are considered loyal are influenced by the organization's formal and informal stance toward such behaviors (K. Smith & Oseth, 1993). Therefore, organizations should champion reporting by actively demonstrating that it is a desired behavior within the organization and reinforce this stance by protecting those who raise issues (Miceli & Near, 1994; Near & Miceli, 1996).

Research Questions

The prior discussion of the existing literature raises the following research questions: (1) *How can system design better protect whistleblower anonymity?*; (2) *How can system design allow for anonymous, two-way communication between the whistleblower and investigator?*; (3) *How can system design improve an investigator's ability to assess whistleblower credibility?* (4) *How can system design increase employees' likelihood of blowing the whistle?*

Research Studies

This dissertation research is comprised of three separate yet related studies on ethics management reporting systems: (1) *The Design of an Anonymous, Two-Way, Ethics Management Reporting System*, (2) *The Impact of Anonymous, Two-Way Communication on Perceived Whistleblower Credibility*, and (3) *Perceptions of Anonymity Protections Provided by Ethics Management Reporting Channels*. The common thread that weaves the essays together into one cohesive dissertation is the role

and importance of anonymity in the design and use of an ethics management reporting system.

CHAPTER TWO

THE DESIGN OF AN ANONYMOUS, TWO-WAY, ETHICS MANAGEMENT REPORTING SYSTEM

Introduction

While there has been a significant number of articles in the media and academic literature focused on whistleblowing (Miceli & Near, 2005), limited research has focused on a critically overlooked component of modern whistleblowing; that is, the reporting system itself. Despite suggestions for, references to and a recognized need for such systems in academic research (Elias, 2008; Hassink et al., 2007; Lowry et al., 2013; MacNab & Worthley, 2007; C. Park & Keil, 2009; Silowash et al., 2012), little to no attention has been given to the necessary requirements for and specific design of effective whistleblowing systems. In order to increase the rate of reporting, it is critical for reporting systems to be designed with the intent to reduce employee fears and inhibitions, while also assisting investigators in determining the credibility and accuracy of reports. Therefore, the primary goal of this chapter is to enhance a firm's ability to solicit and investigate concerns by proposing a modern system design aimed at fostering anonymous, two-way communication between employees and those responsible for investigating wrongdoing within organizations.

Most of the systems currently in use for reporting wrongdoing were developed shortly after passage of the *Sarbanes-Oxley Act* (2002), which requires the implementation of an anonymous reporting channel for all publicly-traded firms in the United States. However, the progression of system development appears to be quite limited since. In fact, most of the recent development has been driven by media organizations, such as the Freedom of the Press Foundation (<https://freedom.press/>). For example, platforms such as WikiLeaks, SecureDrop and GlobaLeaks primarily cater to and encourage the public release of information through various news outlets. Further, SecureDrop and GlobaLeaks are open source projects, which allows for a wide adoption among media organizations.

Research has shown that those who disclose wrongdoing are likely to experience high rates of retaliation. Due to the increase in external channels for reporting wrongdoing, it is critical that firms respond by providing employees with effective and safe channels to internally report issues and concerns in order to reduce the risk of potentially damaging information being released publicly. Therefore, firms must ensure that internal channels provide high degrees of anonymity, otherwise organizations risk employees seeking external channels capable of granting better anonymity protection.

Despite its use in practice, prior research has yet to even suggest the possibility of two-way communication in the context of whistleblowing. Two-way communication is capable of improving the exchange of information between source and investigator, which allows for follow up questions to be asked by the investigator that could lead to additional information to be provided by the whistleblower. Further, two-way communication allows the whistleblower to remain informed of the status of their claim

and any subsequent investigation. Although existing systems have adopted two-way communication capabilities, they fail to provide adequate anonymity protections. In addition, affording whistleblowers with anonymity increases the challenge of investigating claims. Therefore, additional methods and metrics must be incorporated into the design of reporting systems in order to assist investigators in assessing whistleblower credibility.

Despite a steady stream of whistleblowing research over the past 25 years, both literature and practice have yet to benefit from a formal design for an effective anonymous whistleblowing system. In order to meet this need, this chapter proposes the necessary requirements for and a conceptual design of such a system. In doing so, this chapter will employ design science (Hevner et al., 2004; March & Smith, 1995; Walls, Widmeyer, & El Sawy, 1992, 2004) to theorize and justify the design of an anonymous reporting system artifact by building constructs, developing models and explaining the methods necessary to achieve the desired goals of reporting for all actors involved.

Literature Review

This section will provide a review of the relevant literature for the design of an ethics management reporting system. First, design science will be introduced and explained in order to provide an outline of the design process. Second, *ethics management reporting*, along with its four subclasses, will be explained in order to distinguish the differences among various types of disclosure. Finally, theories and methods supporting the use of two-way, anonymous communication will be examined in order to explain its role in the design and use of the proposed ethics management reporting systems.

Design Science

Design science, as opposed to natural science, focuses on the creation of artifacts to attain desired outcomes to problems (Simon, 1988; Walls et al., 2004). A number of articles have established a solid foundation for design science research process. Specifically, March & Smith (1995) organized design science research into activities and outputs, while Hevner et al. (2004) outlined a number of guidelines for conducting design science research, and Walls et al. (1992, 2004) stressed the need for design science to be grounded in theory. As such, this section will provide an overview of design science by reviewing these seminal works.

Activities and outputs. The development of artifacts to accomplish specific tasks is rooted in design science. However, in order to effectively employ design science, one must first understand the necessary activities and desired outputs of such pursuits. March & Smith (1995) developed a research framework which outlines a number of activities and outputs of design science research. The activities in which one would engage while conducting design science research draw from design science and natural science and consist of: (1) *build*, (2) *evaluate*, (3) *theorize*, and (4) *justify*. Building and evaluating are the primary activities of design science while theorizing and justifying are at the core of natural science. The combination of both natural science and design science research perspectives allows for the creation of new artifacts based upon grounded theory in order to solve relevant issues.

The outputs of conducting design science research consist of: (1) *constructs*, (2) *models*, (3) *methods*, and (4) *instantiations*. Constructs are developed in order to provide the vocabulary to be used for a given domain. Therefore, constructs allow

designers to form a conceptualization of the problems within the domain so that potential solutions can be specified. Models express the relationships among constructs through a set of propositions or statements among constructs. The use of models allows designers to represent the situations under examination as problem and solution statements. Each of the activities is briefly described in Table 2.1.

Table 2.1 – Activities of Design Science Research (March & Smith, 1995)

	Item	Description
Research Activities	Build	The construction of the artifact, demonstrating that such an artifact can be constructed. We build constructs, models, methods, and instantiations.
	Evaluate	The development of criteria and the assessment of artifact performance against those criteria. We evaluate artifacts to determine if we have made any progress.
	Theorize	The construction of theories that explain how or why something happens. Determines why and how the artifact worked or did not work.
	Justify	The gathering of scientific evidence that supports or refutes the theory.

Before designers can begin the design process, it is critical to outline the process to be used to achieve the goals of the system. Therefore, methods are outlined in order to provide the steps to be used. Methods are based on the set of underlying constructs and models, which provides a full representation of the solution space. Lastly, after relying upon the constructs, models and methods, designers should ultimately reach a full instantiation of the artifact. In sum, design science is focused on building and evaluating artifacts to achieve desired outcomes, while also theorizing and justifying the design and outcomes of such artifacts. Each of the outputs is briefly described in Table 2.2.

Table 2.2 – Outputs of Design Science Research (March & Smith, 1995)

	Item	Description
Research Outputs	Constructs	Form the vocabulary of a domain. Constitute a conceptualization used to describe problems within the domain and to specify their solutions.
	Models	Set of propositions or statements expressing relationships among constructs. Represent situations as problem and solution statements.
	Methods	Set of steps used to perform a task. Based on a set of underlying constructs and a representation (model) of the solution space.
	Instantiations	The realization of an artifact in its environment. Operationalizes constructs, models, and methods.

Research guidelines. In order to further advance the use of design science, Hevner, March, Park, & Ram (2004) developed a set of guidelines for conducting design science research. The guidelines consist of: (1) *design as an artifact*, (2) *problem relevance*, (3) *design evaluation*, (4) *research contributions*, (5) *research rigor*, (6) *design as a search process*, and (7) *communication of research*. Each of the guidelines is briefly described in Table 2.3. Hevner et al. (2004) also extended prior design science frameworks by illustrating how the suggested research guidelines for conducting design science and the activities and outputs outlined in March & Smith (1995) work in unison to leverage the collective knowledge base in order to solve relevant problems in the business environment. The relationships among the various aspects of design science are illustrated in Figure 2.1.

Table 2.3 – Design Science Research Guidelines (Hevner et al., 2004)

Guideline	Description
Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

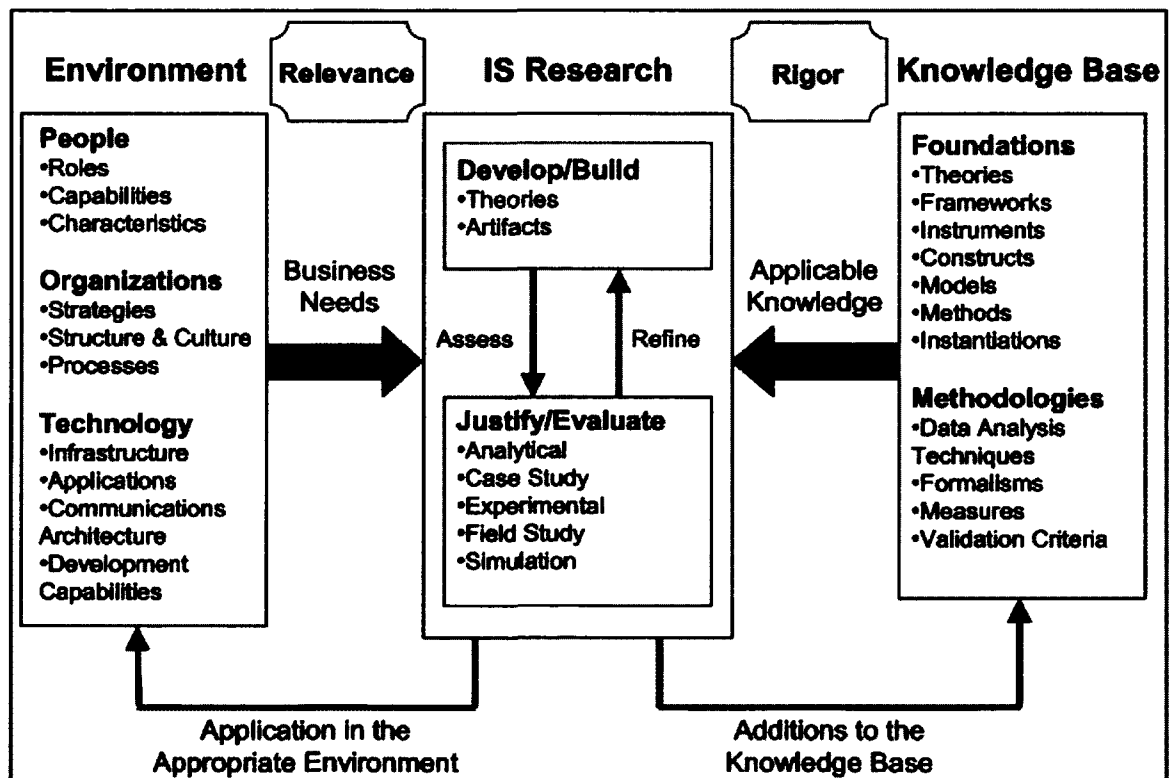


Figure 2.1 – Information Systems Research Framework (Hevner et al., 2004)

Design theory. Walls et al. (1992, 2004) outlined components for information system design theories (ISDT), which views design as both a product and a process. The necessary theory components for a design product consist of the following: (1) *meta-requirements*, (2) *meta-design*, (3) *kernel theories*, and (4) *testable design product hypotheses*. The necessary theory components for the design process consist of: (1) *design method*, (2) *kernel theories*, and (3) *testable design process hypotheses*. The components of information system design theory are briefly described in Table 2.4.

Table 2.4 – Information System Design Theory (Walls et al., 1992, 2004)

	Component	Description
Design Product	Meta-requirements	Describes the class of goals to which the theory applies.
	Meta-design	Describes a class of artifacts hypothesized to meet the meta-requirements.
	Kernel theories	Theories from natural or social sciences governing design requirements.
	Testable design product hypotheses	Used to test whether the meta-design hypotheses satisfies the meta-requirements.
Design Process	Design method	A description of procedure(s) for artifact construction.
	Kernel theories	Theories from natural or social sciences governing design process itself.
	Testable design process hypotheses	Used to verify whether the design hypotheses method results in an artifact which is consistent with the meta-design.

The components of an ISDT are embedded within the information system design process. The kernel theories provide the theoretical foundation for meeting the meta-requirements for a particular system. Each component then lays the foundation for meta-design and the design method. Once the artifact has been designed, the product and process must both be assessed using testable hypotheses. The relationships and dependencies among ISDT components are illustrated in Figure 2.2.

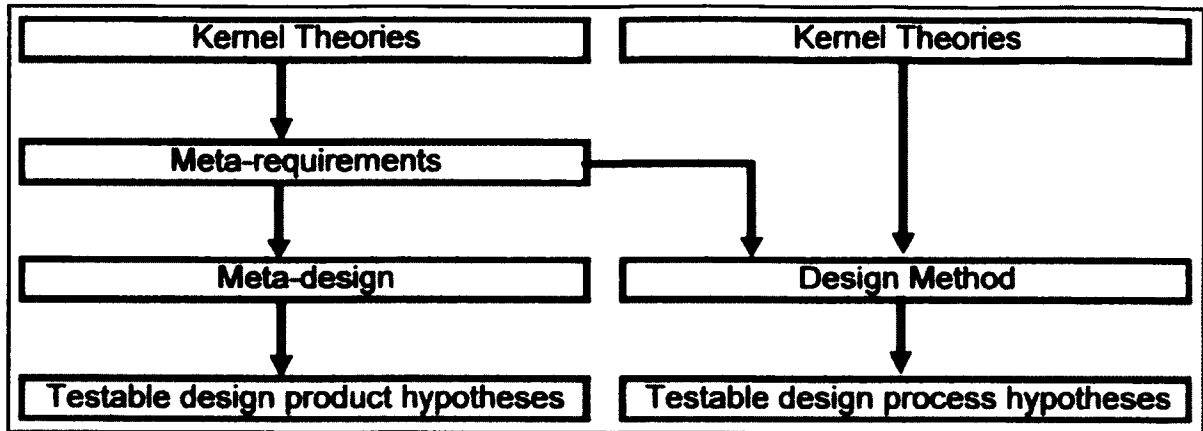


Figure 2.2 – Relationships Among ISDT Components (Walls et al., 1992, 2004)

For the purposes of this design science research, the following design theory components have been identified and outlined for inclusion in the design product and design process for the development of an anonymous, two-way ethics management system (Table 2.5). The meta-requirements for such a system should (1) provide high level whistleblower anonymity, (2) increase the incidence of disclosing wrongdoing, and (3) enhance the accuracy of investigator assessment. In order to meet these requirements, the meta-design will employ a variety of technological components from computer science, such as anonymity measures, data encryption and text-analysis.

Kernel theories will be pulled from reference disciplines, such as communication, management and ethics, in order to establish mental models of the perceived threats and system use cases, as well as assess the effectiveness of the design process. Ultimately, the design product and design process will be assessed by testing formal hypotheses, such as: investigators will more accurately assess whistleblower credibility through two-way communication; users will perceive the proposed system features as providing high degrees of anonymity. However, as the present chapter is only focused on the theoretical

and conceptual system design, these formal tests will be conducted in Chapters 3 and 4 of this dissertation.

Table 2.5 – Design Theory for Anonymous, Two-Way Ethics Management Systems

	Component	Criteria
Design Product	Meta-requirements	System should provide high level whistleblower anonymity, increase the incidence of disclosing wrongdoing, and enhance the accuracy of investigator assessment
	Meta-design	Anonymity measures, Encryption, Text-analysis
	Kernel theories	Computer science, Communication, Management and Ethics
	Testable design product hypotheses	Users will perceive the system to provide high level anonymity; investigators will more accurately assess whistleblower credibility
Design Process	Design method	Existing systems and emerging technology will be assessed and considered for inclusion into the design of ethics management systems
	Kernel theories	Communication, management and ethics theories
	Testable design process hypotheses	The assessment of the system by potential whistleblowers will provide testable hypotheses for the design

Ethics Management

Before initiating the design process, it is essential that key concepts and terms are clearly established. While the term *whistleblowing* is often widely applied to any disclosure of wrongdoing, it is important to distinguish the key differences among four types of disclosures, or *ethics management reporting* (Table 2.6): (1) *internal reporting*, (2) *external reporting*, (3) *internal whistleblowing*, and (4) *external whistleblowing* (MacNab et al., 2007). Regardless of whether the disclosure is made internally or externally, the primary distinction between reporting and whistleblowing is that reporting is conducted through organizationally authorized channels, whereas whistleblowing occurs when an employee does not follow the organization's official reporting policy.

Table 2.6 – Typology of Ethics Management Reporting (MacNab et al., 2007)

Type	Features	Outcomes for Organization	Outcomes for Whistleblower	Example
Internal Reporting¹	Authorized by target organization Reported within target organization Organizationally proactive (ethics management proactive/responsive)	Knowledge of wrongdoing remains internal Opportunity to correct wrongdoing	Threat of retaliation Wrongdoing may not be properly investigated Required for most in order to receive legal protection	An employee reports the improper organizational accounting practices via an established ethics hotline or to an established, internal ombudsman.
External Reporting	Authorized by target organization Reported externally in relation to the target organization Organizationally proactive (ethics management proactive/responsive)	Knowledge of wrongdoing is not made public, but is no longer internally controlled	Reduced threat of retaliation due to independent investigator Increased likelihood of effective investigation	An employee reports the improper organizational accounting practices to an organizationally endorsed, third party such as an external auditor or ethics consultant.
Internal Whistleblowing	Unauthorized by target organization Reported within target organization Organizationally passive (ethics management passive/reactive)	Knowledge of wrongdoing is not made public, but is no longer handled within the established procedure	Increased threat of retaliation	An employee unexpectedly announces the improper organizational accounting practices during a board of directors meeting.
External Whistleblowing²	Unauthorized by target organization Reported externally in relation to target organization Organizationally passive (ethics management passive/reactive)	Allegations of wrongdoing are made public Increased potential for strategic, financial and/or legal consequences	Highest threat of retaliation Allows for greatest pressure on organization to correct wrongdoing	An employee communicates the improper organizational accounting practices directly to the SEC or other government regulatory body.

1 – most desired by organizations

2 – least desired by organizations

While some ethicists have argued that directly confronting the alleged wrongdoer(s) is the only moral option initially available to an employee who wishes to correct misconduct (Bowie, 1982; DeGeorge, 1986; Velasquez, 2005), others have reasoned that electing to use other channels is acceptable under certain conditions, such as if the employee perceives a threat of retaliation or when first attempts to solve the issue prove to be unsuccessful (Kaptein, 2002; Larmer, 1992; Miceli & Near, 1992). Therefore, while the ordering of each type of ethics management reporting is consistent with a logical progression from most to least desirable (i.e., from authorized to unauthorized and internal to external), some employees may elect to skip one or more of the channels due to a fear of retaliation and/or a culture of organizational silence, both of which will be discussed later in greater detail.

Internal reporting. Internal reporting occurs when an employee utilizes an organization's officially authorized channel to report wrongdoing to an empowered entity within the organization itself. Authorized channels are communicated to employees through an organization's policies, procedures and/or training. An example of internal reporting would include the reporting of misconduct using an authorized internal reporting channel, such as open door policies, an ethics ombudsman or telephone hotline (Kaptein, 2002). While establishing an internal reporting channel for employees is only explicitly required for publicly traded firms in the United States, private firms would be wise to voluntarily implement internal reporting policies, procedures and systems.

External reporting. External reporting is also authorized by the organization, but allows for reports to be received by an outside entity, such as independent auditors or third-party compliance firms. Although reporting to an independent entity outside of the

organization may be perceived as more credible by employees and can allow for increased employee anonymity and confidentiality, external reporting can also result in a decrease in investigation efficiency due to the investigator's reduced knowledge of the inner workings of the organization (Kaptein, 2002). An excellent example of organizationally-approved external reporting would be the sharing of actionable information as it pertains to threats, vulnerabilities, and incidents with an industry's Information Sharing and Analysis Center (ISAC).

Internal whistleblowing. Internal whistleblowing is classified as reporting conducted within the organization, but via unauthorized channels. An example of internal whistleblowing would be when an employee does not follow an organization's policy of first reporting any concerns to his or her direct supervisor and instead elects to inform higher management. While an organization can still maintain control over a case of internal whistleblowing, the likelihood of retaliation may increase since the employee elected to not follow the established reporting procedure.

External whistleblowing. External whistleblowing occurs when an employee elects to disclose misconduct to an outside party that the organization has not endorsed, such as the media, a government agency, a non-governmental organization, or a professional organization (Kaptein, 2010). From an organization's perspective external whistleblowing can be a manager's nightmare as it is viewed as a breach that is likely to lead to negative publicity, regulatory investigations, and legal liability (Barnett et al., 1993). Rothschild & Miethe (1999) found that employees are more likely to resort to external whistleblowing "once they come to believe that internal channels are closed to them, that the organization is not moral, and that senior management is inert or complicit

in the wrongdoing.” Consistent with these findings, Sims & Keenan (1998) concluded that supervisor support, informal policies, gender, and ideal values are significantly related to external whistleblowing. Therefore, the culture of the organization is critical to reducing the incidence of external whistleblowing.

For the sake of simplicity, unless a particular type of reporting or whistleblowing is specified, any future use of the terms “whistleblowing” or “whistleblower” in the remainder of this dissertation are to be interpreted in a general sense and refer to all types of ethics management reporting, unless a specific type is explicitly stated.

Two-Way Communication

Early models of communication (Berlo, 1960; Shannon, 1948) are limited to one-way communication due to the unidirectional nature of such transmissions. Common examples of one-way communication consist of radio and television, as the audience cannot respond to the broadcast. Thus, the inability for the receiver to communicate with the sender in one-way transmissions may result in a breakdown in communication as the sender cannot verify that the receiver properly received or understood the message.

Barnlund's (1970) addition of feedback to earlier models helps address this issue. This reciprocal, two-way communication method allows for a more thorough exchange of information as the receiver can provide feedback to the sender in order to ask for clarification or confirmation of the original message. An illustration of Berlo's (1960) Sender-Message-Receiver-Channel (SMRC) Communication Model, with the inclusion of Barnlund's (1970) feedback, is provided in Figure 2.3. Note that Barnlund (1970) does not explicitly designate a sender or receiver since both parties can dynamically alternate between both roles as many times as necessary to complete the communication exchange.

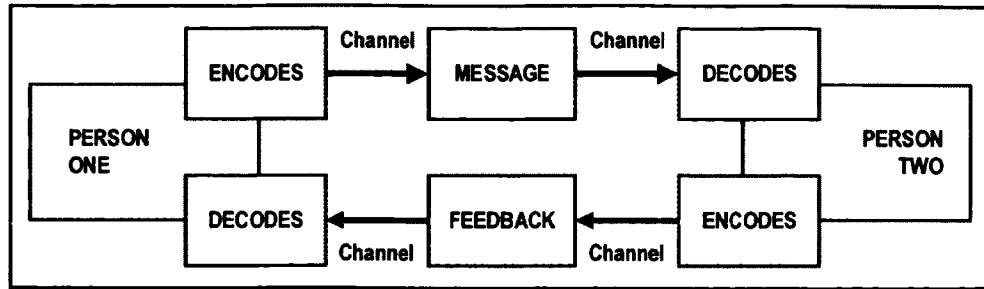


Figure 2.3 – Addition of Barnlund’s (1970) Feedback to Berlo’s (1960) SMRC Model

The use of feedback also allows the receiver to communicate, both verbally and nonverbally, with the original sender in response to his or her message. For example, facial expressions and body language can provide the sender with nonverbal behavioral cues from the receiver, which informs the sender of communication effectiveness.

Barnlund's (1970) original transactional communication model is illustrated in Figure 2.4.

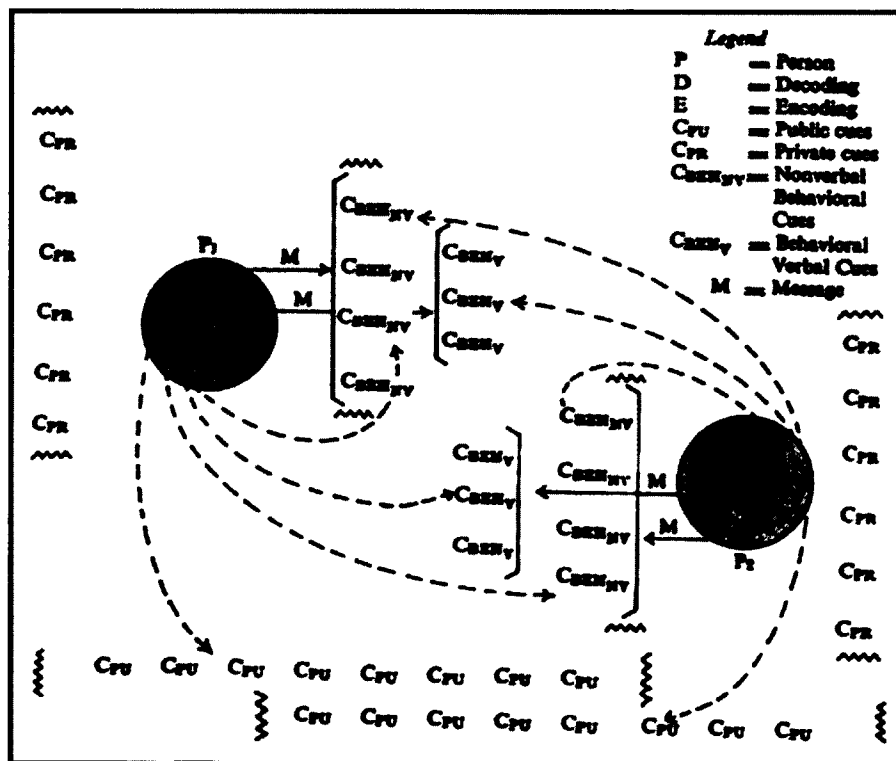


Figure 2.4 – Barnlund’s (1970) Transactional Model of Communication

With respect to whistleblowing, two-way communication provides both whistleblowers and investigators the opportunity to exchange additional information relevant to the investigation. For example, a whistleblower may neglect to, whether intentionally or unintentionally, provide insight that is critical to the investigation. Two-way communication would allow for the investigator to ask the whistleblower to clarify information already received or request more information to aid in the investigation. Further, two-way communication allows for whistleblowers and investigators to develop a rapport, which is helpful in establishing and maintaining trust.

Anonymity, Unlinkability, and Undetectability! Oh, my!

In addition to the need for two-way communication, anonymity is also critical in order to protect whistleblowers from retaliation. However, before discussing anonymous communication in general, it is useful to establish clear definitions of terms relevant to anonymity. A decade-long collaboration on Pfizmann & Hansen's (2010) working paper provides us with a number of terms with highly refined definitions, such as: *anonymity*, *unlinkability*, *undetectability*, and *unobservability*. These terms and their related definitions are provided in Table 2.7.

Table 2.7 – Definitions Related to Anonymity (Pfitzmann & Hansen, 2010)

<i>Anonymity</i> of a subject from an attacker’s perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set.
<i>Unlinkability</i> of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker’s perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not.
<i>Undetectability</i> of an item of interest (IOI) from an attacker’s perspective means that the attacker cannot sufficiently distinguish whether it exists or not.
<i>Unobservability</i> of an item of interest (IOI) means: <ul style="list-style-type: none"> • undetectability of the IOI against all subjects uninvolved in it; and, • anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI

Anonymity means that an interested party cannot identify an individual subject among the set of possible users (i.e., the anonymity set). On the other hand, identifiability indicates that the subject can be identified within the anonymity set and therefore no longer maintains any degree of anonymity from an interested party. Obviously, it is in the best interest of those who disclose wrongdoing to maintain anonymity when communicating with investigators in order to limit the likelihood of retaliation.

An item of interest, such as a user, message or action, is considered unlinkable if an attacker cannot connect it to another item of interest. Conversely, if an attacker can determine that an item of interest is related to another, the item is considered linkable. Unlinkability essentially provides an individual with plausible deniability with respect to who reported an alleged wrongdoing. However, if only a few individuals aware of the wrongdoing, the disclosure will be the more linkable due to the smaller anonymity set.

Undetectability refers to whether an attacker can determine whether an item of interest even exists. This is certainly desirable in the context of whistleblowing as an attacker is forced to cast a wide net and cannot target a specific user, system or transmission.

Unobservability requires that the item of interest be both undetectable with respect to those uninvolved with the transmission while also remaining anonymous to those who are involved. Designing a system that can achieve unobservability provides the greatest protection for both anonymity and security. Therefore, it is the goal of the proposed system to achieve unobservability.

Onion Routing

Onion routing is an anonymous communications protocol that serves as the fundamental concept for what is now simply known as Tor (The Onion Router). Onion routing was first developed in the mid-1990s by Goldschlag, Reed, & Syverson (1996), while all were employed by the U.S. Naval Research Laboratory, in an effort to anonymize the intelligence communications of the U.S. military. The use of onion routing allows for low-latency communications to be relayed among multiple nodes on the Internet prior to reaching the intended destination, which prevents the destination from knowing the IP address of the sending device. This is achieved by wrapping the transmission data in multiple layers of encryption, with each layer of the proverbial onion peeled off in succession by each of the intended relays comprising the onion routing circuit. Each layer of encryption only contains the IP address for the next node in the circuit so that no single node has knowledge of anything beyond who sent the packet and where it should be forwarded. As long as the circuit is comprised of at least three nodes, no single node can determine the full path of the circuit. Goldschlag, Reed, & Syverson's (1996) conceptualization of onion routing is reproduced in Figure 2.5.

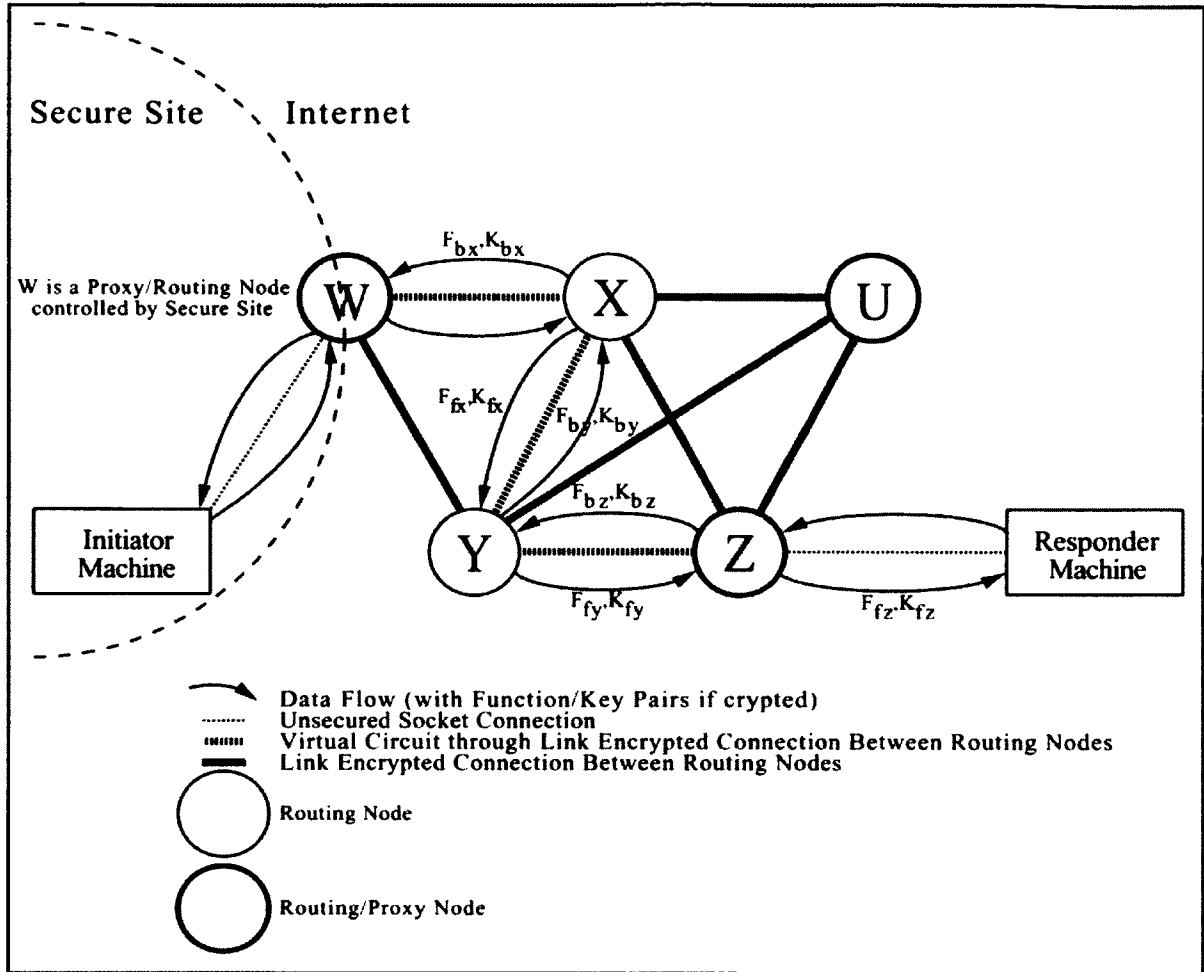


Figure 2.5 – Onion Routing (Goldschlag, Reed, & Syverson, 1996)

Existing Reporting Channels

A number of channels have been used to solicit reports of wrongdoing, with postal mail being the most rudimentary and telephone hotlines being the most common (Weaver, Trevino, & Cochran, 1999). However, the advent of the Internet has allowed for the use of other channels, such as web forms and e-mail. This section will outline the benefits and limitations of each in greater detail.

Open door policy. The intent of an open door policy is to encourage employees to speak to members of management rather than withhold information by remaining silent.

However, the extant research in this area shows how such policies might not produce the desired results if organizational culture does not match what is said in the employee handbook. As one might expect, employees are naturally hesitant to share negative news or opinions with management (Detert & Burris, 2007; Detert & Trevino, 2010; Miceli & Near, 1994; Morrison & Milliken, 2000), especially if it might reflect poorly on their standing within the organization (C. Park & Keil, 2009; Rosen & Tesser, 1970; H. J. Smith & Keil, 2003; Wang, Keil, & Wang, 2015). Most importantly, it is impossible to disclose wrongdoing anonymous via an open door policy and the most an employee can hope to achieve is confidentiality. However, even if confidentiality is achieved, it is not sufficient to protect against the threat of retaliation.

Postal mail. The disclosure of wrongdoing through postal mail allows for whistleblowers to maintain high levels of anonymity provided that he or she cannot be identified at the time of mailing. However, without providing a return address or contact information for the investigator, anonymous, two-way communication is impossible through this channel.

Telephone. According to Weaver et al. (1999), 51% of Fortune 1000 firms had adopted telephone-based hotline systems for employees to raise complaints before the turn of the century. Over a third of the hotlines were directed to employees of the organization's ethics or compliance office. Legal teams and audit departments also fielded a large percentage of calls to organizational hotlines (19% and 18%, respectively). They further report that other departments and external parties were recipients of hotline reports (human resources, 8% of firms; security, 4%; external consultants, 9%; and miscellaneous other functions or combined functions, 8%). However, a survey conducted

by the nonprofit Ethics Resource Center (2010) revealed that only three percent of reports about internal misconduct come to company hotlines, with an organization reporting that an average of 431 hotline tips are submitted every month, with almost 20 percent of these lead to findings of misconduct.

The use of telephone hotlines provides whistleblowers with a convenient method of reporting wrongdoing while also allowing clear and efficient two-way communication. However, telephone hotlines are unlikely to provide any degree of reasonable anonymity protection without additional action on the part of the whistleblower. Firstly, the use of any audible communication channel to report wrongdoing is susceptible to voice analysis. Secondly, phone calls are easily traced and likely reveal the caller's phone number through standard caller ID services. While determining the physical location of a mobile phone takes additional effort and technology, a phone number is all that is needed to identify a large portion of the population.

Fax. Although unlikely to be the first choice for most whistleblowers, it is possible to submit a report of wrongdoing via fax. While there are more efficient means for reporting wrongdoing, the use of a fax machine would allow for the transmission of evidence in order to provide supporting documentation for the alleged claims. However, just as with the telephone, faxes are easily traceable and can reduce the whistleblower's level of anonymity.

Web forms. The Internet has allowed for wrongdoing to be reported in a variety of new ways. The use of online forms to collect desired information from individuals is a standard practice in today's digital age. A primary advantage for the use of web forms is that it allows for the recipient to prompt the sender for relevant information using form

elements such as text fields, check boxes and radio buttons. However, standard use of online technology leaks information about the identity of the user. Therefore, a naïve user who submits his or her allegations through an online web form may result in the whistleblower unintentionally revealing information that can be used to determine his or her identity.

Email. Some organizations have encouraged employees to submit wrongdoing via e-mail. While this channel does provide convenient and efficient two-way communication, if the user does not take additional steps to obfuscate his or her identity, e-mail does not provide any reasonable level of anonymity protection for a whistleblower concerned with the threat of retaliation.

A brief outline of the advantages and disadvantages for each reporting channel is provided in Table 2.8. Note that the comparisons have been made under the assumption of a naïve user. Therefore, the channels are assessed in the context of common usage and do not account for additional measures one might employ to increase his or her anonymity when communicating via such channels.

Table 2.8 – Existing Reporting Channels

Reporting Channel	Advantages	Disadvantages
Post Mail	High anonymity Transmission of physical evidence/documents	No return address prevents two-way communication High latency transmission
Telephone Hotline	Low latency transmission Two-way communication during the initial report	Traceable Voice analysis Lowest anonymity
Fax	Transmission of physical evidence/documents	Traceable Limited access
Web Form	Low latency transmission Prompts for desired information	Traceable Low anonymity
Email	Low latency transmission Two-way communication	Traceable Low anonymity

NOTE: The advantages and disadvantages for each channel are provided in the context of common usage and do not account for additional measures one could take to increase anonymity when using such channels.

Existing Reporting Systems

Before advocating for a particular system design, it is important to first review the existing systems currently available. A number of dedicated reporting systems have been developed to address the needs of organizations. For example, as many as 35 or more companies entered the market in response to the requirements of Sarbanes-Oxley (Green, 2004; Jones, 2003). However, upon review, it appears that most of the proprietary systems available on the market fail to achieve adequate anonymity protection. A detailed review of existing reporting systems was conducted as part of this research and can be obtained from the author. A brief overview of each of these systems is provided in Table 2.9.

Table 2.9 – Existing Reporting Systems

System	Primary Developer	Primary Report Type						Report Channel				Two Way Comm.	Development	
		IR	ER	IW	EW	P	W	E	F	M				
BKMS-Z	Business Keeper AG	X						X					X	Proprietary
BKMS-D	Business Keeper AG	X						X					X	Proprietary
BKMS-O	Business Keeper AG		X					X					X	Proprietary
ClearView Connects	ClearView Strategic Partners, Inc.		X					X					X	Proprietary
EthicsPoint	NAVEX Global	X						X						Proprietary
Expolink	D3 Security		X					X						Proprietary
Fulcrum Inquiry	Fulcrum Inquiry		X					X						Proprietary
GlobalLeaks	Hermes Center	X	X	X	X			X					X	Open
GRC Suite	The Network, Inc.	X						X						Proprietary
Lighthouse	Lighthouse Services, Inc.	X						X	X	X	X			Proprietary
SecureDrop	Freedom of the Press Foundation				X			X					X	Open
Whistleblower Hotline	NASDAQ OMX		X					X						Proprietary

NOTE:
Report Types: **IR** = Internal Reporting; **ER** = External Reporting; **IW** = Internal Whistleblowing; **EW** = External Whistleblowing
Report Channels: **P** = Phone; **W** = Web Form; **E** = E-mail; **F** = Fax; **M** = Post Mail

Threat Analysis

The design of an effective anonymous internal reporting system is complicated by the sensitive and competing perspectives of the actors involved: potential whistleblowers, investigators and the organization. Therefore, the following sections will discuss the potential threats facing each camp of actors with respect to the context of ethics management reporting.

Organizational Insiders

Those who elect to disclose wrongdoing are likely to experience threatened or actual retaliation (Rothschild & Miethe, 1999). From a potential whistleblower's perspective, the internalized motivation to report an observed wrongdoing is met with concerns about how his or her report will be received by the organization. Unfortunately, these concerns are not unfounded. Employees may perceive that an organization views whistleblowers as disloyal employees and a fear of possible retaliation discourages internal whistleblowing. While the remedy to the uncertainty around loyalty is best addressed by management practices (Near & Miceli, 1996), the threat of retaliation can be diminished, if not eliminated, through the use of proper anonymity measures (Liyanarachchi & Newdick, 2008).

Organizations

Naturally, all organizations would prefer to completely avoid both internal and external whistleblowing. With respect to reporting, two perspectives emerge that an organization may hold with respect to the disclosure of wrongdoing; that is *pro-reporting* and *anti-reporting*. From a pro-reporting organization's perspective, the need to uncover and correct unethical or illegal conduct within the organization is paramount. An

organization in this camp will attempt to eliminate communication barriers between employees and management in order to create a culture of open communication, and reprimand those who interfere with such attempts.

Conversely, anti-reporting organizations are focused on discouraging and suppressing negative reports. For example, a highly autocratic organization might adopt this stance in an attempt to maintain absolute control over the dissemination of organizational information within the organization as well as what is released externally. This may lead organizations to attempt to identify employees who allege wrongdoing anonymously. As discussed earlier, while this approach may prove effective in reducing internal reporting, it often backfires as it is more likely to result in employees resorting to external whistleblowing in the future. Unfortunately, addressing the concerns of organizations who are completely opposed to the thought of reporting is outside of the scope of this research.

Investigators

From an investigator's perspective, anonymous disclosures of wrongdoing might limit his or her ability to collect credible, detailed and actionable evidence of wrongdoing (Near & Miceli, 1995, 1996). Therefore, additional measures must be taken to assist those charged with investigating anonymous reports. Further, investigators are often employees of the organization in question, such as internal auditors, compliance officers or general counsels. The inherent conflict of interest in the relationship between an internal investigator and organization has the potential to suppress prohibitive voice, which is likely to reduce the incidence of internal reporting. While beyond the scope of this research, the use of an independent third party responsible for receiving,

documenting and relaying reports to the organization is suggested in order to provide greater autonomy for the investigator, as well as enhanced anonymity protection for the whistleblower.

Internal investigators may also feel pressured by the organization to downplay the severity or significance of alleged wrongdoing in order to protect the organization from negative consequences. Therefore, in order to ensure a thorough independent investigation is possible, it is suggested that investigators be employed by outside entities, such as compliance firms. However, the nature of this contractual relationship does not completely remove the possibility of an investigator being influenced by his or her manager to suppress certain allegations in order to protect the business relationship between the compliance firm and the client organization.

Attackers

In the context of whistleblowing, all attackers are likely to be interested in identifying or locating users in order to determine the individual(s) responsible for reporting or investigation an alleged wrongdoing. Individuals or organizations accused of wrongdoing might desire to silence the reporting of the wrongdoing itself, while others might be interested in gathering negative information on offending organizations. Regardless of an attacker's motive or relation to a whistleblower, wrongdoer, organization or investigator, we must assume that the adversary has one or more of the following goals: (1) identify or locate users, (2) track user activities on the Internet, (3) eavesdrop on communications in transit, or (4) recover sensitive data after system shutdown.

If an attacker succeeds in identifying or locating a user, the user is likely to experience undesirable outcomes. As discussed earlier, the probability of whistleblowers experiencing some form of retaliation is extremely likely, which makes the preservation of anonymity the primary goal. Further, attackers may attempt to intercept or recover information by eavesdropping on communications or by analyzing a system suspected of being used to electronically communicate wrongdoing. If an attacker succeeds in obtaining such information, it will likely identify the alleged wrongdoer(s), but it might also identify the whistleblower. Therefore the security of such communications must also be of primary concern in order to support the goal of preserving whistleblower anonymity.

In protecting against such attempts, system developers must assume that attackers are highly skilled and are capable of performing highly technical attacks, such as those outlined in the threat model for Tails (The Amnesic Incognito Live System, 2015), which is reproduced in Table 2.10. Therefore, each of these capabilities should be kept in mind during the design, development and implementation of such a system.

Table 2.10 – Capabilities, Methods and Other Means of the Attacker (The Amnesic Incognito Live System, 2015)

Capability	Description
Eavesdropping and content injection	It is assumed that the adversary is non-global and has full control over the network traffic of some portion of the Internet (e.g. some Tor exit nodes, upstream routers of exit nodes, or the ISP that provides the Internet connection the user is sitting behind). The adversary is thus able to eavesdrop, modify, delete or delay parts or all of the user's traffic on the Internet.
Bypass attacks	It is conceivable for attackers to mount attacks which bypass the proxy and DNS setup in the applications which could then be used to identify the user, either by injecting data or social engineering.
Exploit software vulnerabilities	The attacker might be able to run arbitrary code by exploiting vulnerabilities present in any of the software packages installed.
Application level attacks	The attacker can utilize certain applications' services and features to get identifying information. Examples are JavaScript and Java applets in web browsers, CTCP queries in IRC clients, etc.
Physical access, live monitoring, post-mortem equipment analysis	Some users face adversaries with intermittent or constant physical access to the equipment they use. Users in Internet cafes, for example, face such a threat. This means the adversary might be physically monitoring the computer while the PELD is running on it. Moreover the adversary might raid the user at any moment and then confiscate and analyze the equipment, storage media and memory in particular.

Research Questions

This review of the literature, existing reporting systems and threat analysis raises the following primary research questions: (1) *How can reporting system design better protect whistleblower anonymity?* (2) *How can reporting system design allow for anonymous, two-way communication between the whistleblower and investigator?* (3) *How can an investigator's ability to assess whistleblower credibility be improved when using an anonymous reporting system?* With these questions in mind, the remainder of this chapter will propose a system design and explain the features necessary to support the reporting of wrongdoing in a safe and effective manner.

Design Principles

Prior to developing a proposed design for any system, it is wise to establish a set of principles by which the design process can be guided. As such, it is argued that the design of an ethics management system should preserve the user freedoms espoused by *free software*. Further, the proposed system should also satisfy the principles for cryptography espoused by Kerckhoffs (1883).

Free Software

Free software is primarily focused on respecting users' freedom and does not necessarily mean that the software is provided without cost. According to the Free Software Foundation (2015), free software means that "users have the freedom to run, copy, distribute, study, change and improve the software." Therefore, to be considered free software, it must respect four essential user freedoms (Table 2.11): (0) the freedom to run the program as you wish, for any purpose; (1) the freedom to study how the program works, and change it so it does your computing as you wish; (2) the freedom to redistribute copies so you can help your neighbor; (3) the freedom to distribute copies of your modified versions to others.

Table 2.11 – Essential Freedoms of Free Software (Free Software Foundation, 2015)

Freedom	Description
0	The freedom to run the program as you wish, for any purpose
1	The freedom to study how the program works, and change it so it does your computing as you wish. Access to the source code is a precondition for this.
2	The freedom to redistribute copies so you can help your neighbor.
3	The freedom to distribute copies of your modified versions to others. By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

In order to satisfy the requirements of freedoms 1 and 3, all free software must make the source code available for review. While all of the freedoms espoused by the Free Software Foundation are worthy pillars for the development of all systems, the proposed system needs to guarantee such freedoms in order to ensure transparency. Complete transparency is necessary due to the sensitive nature of whistleblowing and the high level of risk many whistleblowers assume in disclosing wrongdoing. Without the ability to thoroughly review the source code, those who wish to come forward and disclose wrongdoing cannot trust that the system will provide adequate anonymity protection or ensure that it has not been compromised in an effort to turn the system into a “honey pot.”

In adherence with these freedoms, all of the technical capabilities necessary for the proposed system can be achieved through the use of free software. Specifically, software such as the Tor Anonymity Network, The Amnesic Incognito Live System (Tails), and the Metadata Anonymization Tool (MAT) are all available in accordance with the free software definition. Each of the aforementioned software may also be downloaded and utilized without cost, although it is not required in order to be considered free software.

Kerckhoffs' Principles for Cryptography

In what is considered one of the most complete, yet concise, works on cryptography, Auguste Kerckhoffs (1883) outlines six principles which must be considered prior to selecting a field cipher. Kahn's (1996) translation of these principles from French to English is reproduced in Table 2.12, and outlined as follows: (1) the system should be, if not theoretically unbreakable, unbreakable in practice;

(2) compromise of the system should not inconvenience the correspondents; (3) the key should be rememberable without notes and should be easily changeable; (4) the cryptograms should be transmittable by telegraph; (5) the apparatus or documents should be portable and operable by a single person; (6) the system should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.

Table 2.12 – Kerckhoffs’ Principles for Cryptography (Kahn, 1996, p. 235)

Principle	Description
1	The system should be, if not theoretically unbreakable, unbreakable in practice.
2	Compromise of the system should not inconvenience the correspondents.
3	The key should be rememberable without notes and should be easily changeable.
4	The cryptograms should be transmittable by telegraph.
5	The apparatus or documents should be portable and operable by a single person.
6	The system should be easy, neither requiring knowledge of a long list of rules nor involving mental strain.

Although Kerckhoffs’ principles were intended for cryptograms, they serve as useful guidelines for all aspects of systems which intend to protect the transmission of sensitive information. While satisfying all six principles can be quite challenging, each of the technological measures included in the proposed design is intended to meet or exceed one or more of Kerckhoffs’ principles.

Proposed System Design

An illustration of the proposed system design is provided in Figure 2.6. While an organization can employ the proposed system for each of the four types of ethics management reporting, the illustration is geared towards external reporting. Further, the

design is largely based upon the architecture of the SecureDrop system, as the features and methods of that system currently provide the highest performance guarantees in terms of anonymity and security. Each of the system features in the illustration, as well as others not depicted, will be discussed in detail in the following sections.

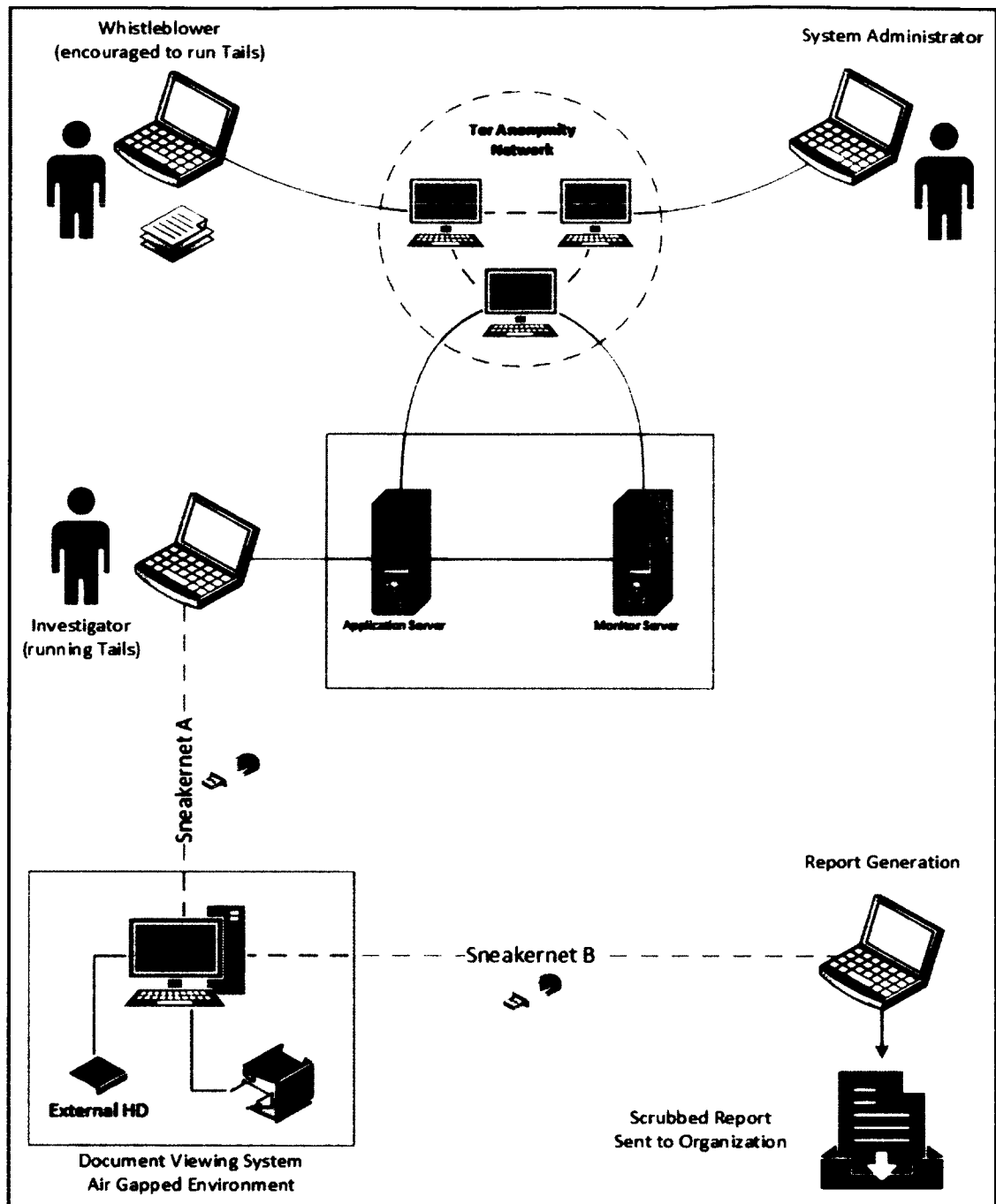


Figure 2.6 – Overview of the Proposed System Design

The illustration includes the following users: whistleblower, investigator and system administrator. Prior to accessing the system, both whistleblowers and investigators are encouraged to use The Amnesic Incognito Live System (Tails) to

increase user anonymity and security. All transmissions to and from the users of the system are encrypted from end-to-end prior to being routed through the Tor Anonymity Network. The encrypted communications and any relevant documents accompanying a message must be extracted and transported from the server to a document viewing station equipped with a system not connected to the Internet. Further, the use of a secure, air-gapped environment, ideally protected by a Faraday cage, ensures that the contents of each transmission is only viewable within the authorized area.

After investigators review the information provided in the transmission, they may communicate with the whistleblower to request additional information. Prior to extracting the necessary information to compile a report of the wrongdoing, all potentially identifying information should be scrubbed from the documents and information provided in order to protect the whistleblower. After doing so, the information relevant to the report may be extracted from the secure viewing station to another system outside of the document viewing area. Investigators may then generate the report intended to be sent to the organization in order to inform them of the allegations and subsequent investigation.

System Use Case

The system use case for interacting with system is fairly straight-forward and is illustrated in Figure 2.7. A user wishing to report a given wrongdoing for the first time will submit their information via the system. After submission, the user will be provided with a system-generated passphrase comprised of random words. It is critical that the user commit the passphrase to memory and not compromise its secrecy as it is the only means by which a user can access a prior submission. Upon returning to the system, existing

whistleblowers simply enter the passphrase associated with their original report to check the status of their case and to view and respond to any messages provided from an investigator.

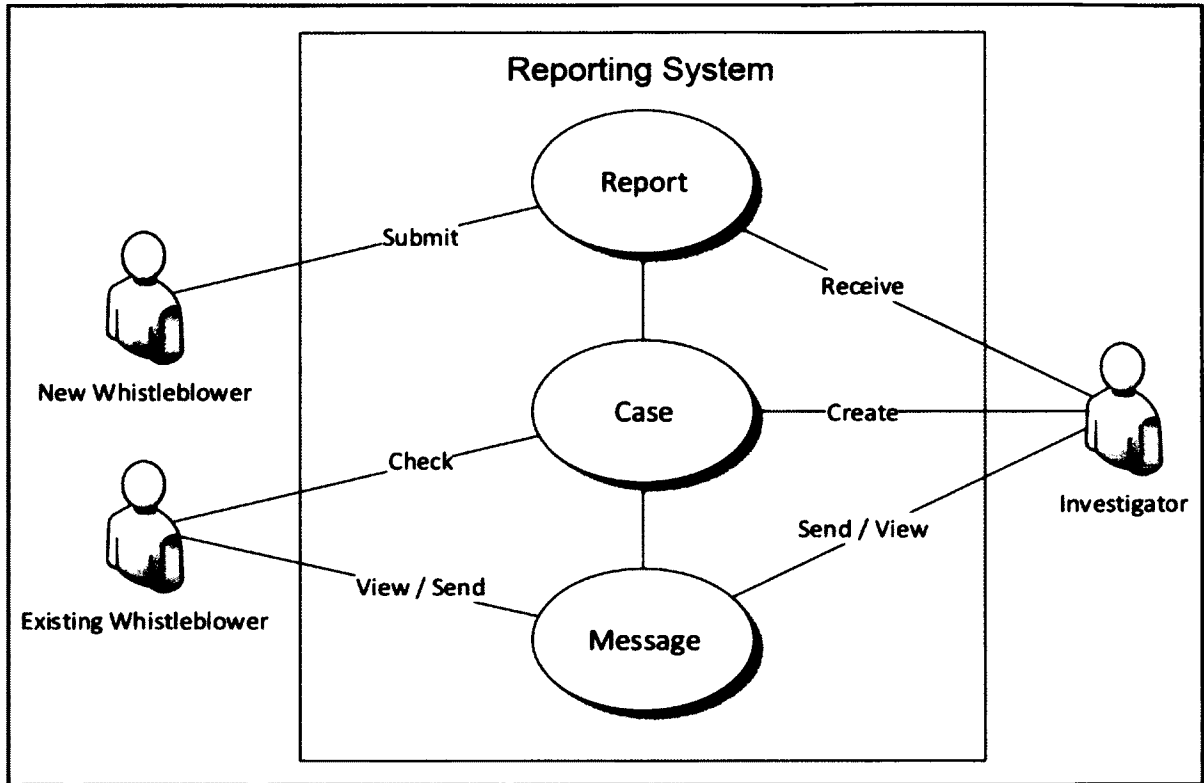


Figure 2.7 – Use Case for the Proposed System

Upon receipt of a new report, the investigator may create a case and review the information provided by the whistleblower. The use of a case allows for all of the messages to be associated with a single whistleblower, as well as communicate the status of the investigation. Investigators may send messages to the whistleblower in order to clarify aspects of the submission and to request additional supporting information deemed relevant to the investigation.

System Features

In order to best satisfy the desires of each camp of actors while also fostering effective reporting, the following primary features of an anonymous, two-way ethics management reporting system will be proposed. The system features consist of: (1) data encryption, (2) the Tor Anonymity Network, (3) The Amnesic Incognito Live System (Tails), (4) metadata anonymization, (5) user identification and authentication, (6) two-way anonymous messaging, (7) investigation status, and (8) text analysis. Aside from investigation status, each of the features can be organized into three primary functional categories: security, anonymity and credibility (Table 2.13).

Table 2.13 – Proposed Features of Ethics Management Reporting Systems

Feature	Description	Security	Anonymity	Credibility
Free Software	System should adhere to the principles of Free Software. Source code should be made publicly available to provide maximum transparency and ensure that the system is designed and will perform as intended.	✓	✓	
Data Encryption	Encryption protects the content of the report and communication between whistleblower and investigator from being read by anyone other than the intended recipient.	✓	✓	
Tor Anonymity Network	The Tor Anonymity Network provides enhanced anonymity for the whistleblower and system server by routing communications through a distributed proxy network of relays without revealing IP addresses.	✓	✓	
The Amnesic Incognito Live System (TAILS)	TAILS is a live operating system that aims to preserve user privacy and anonymity. It allows for anonymous use of the Internet on any computer and leaves no trace without explicit authorization.	✓	✓	
Metadata Anonymization	The removal of metadata from files uploaded to support a report of alleged wrongdoing helps protect anonymous whistleblowers by preventing their identity from being unintentionally revealed.	✓	✓	
User Identification and Authentication	Whistleblowers should only be provided with a system-generated passphrase in order to protect anonymity. Investigators may only be granted access to the system after satisfying multifactor authentication.	✓	✓	✓
Two-Way Anonymous Messaging	Anonymous two-way messaging between the whistleblower and investigator allows for additional information or evidence to be shared in order to assist the investigation and establish whistleblower credibility.		✓	✓
Investigation Status	Providing the whistleblower with the current status of the investigation within the system is critical since an anonymous whistleblower cannot be notified of updates through regular communication channels (e.g., e-mail, phone).			
Text-Analysis	Text-analysis algorithms designed to detect deception and assess credibility can provide investigators with an objective credibility rating of report content.			✓

Data Encryption

Data encryption involves the use of algorithms to obfuscate the true meaning of content. The development of encryption standards assumes that such information can and will be intercepted. Therefore, encryption is used solely to ensure that the content of sensitive information is not accessible by those unauthorized to view it. There are three types of encryption algorithms: (1) *symmetric*, (2) *asymmetric*, and (3) *hashing*. Each of these algorithm types, as well as the concept of *forward secrecy*, will be discussed.

Symmetric algorithms. Symmetric algorithms are designed to use the same secret key for both encrypting and decrypting data. Examples of symmetric encryption include the Data Encryption Standard (DES), Advanced Encryption Standard (AES), and the International Data Encryption Algorithm (IDEA). Because the use of symmetric encryption requires sharing the same secret with those involved in the conversation, a separate key must be generated for each conversation. Otherwise, the holder of a secret key for one conversation could decrypt the contents of another. The need to generate a separate secret key for each and every conversation is one of the major disadvantages of symmetric encryption. However, the simplicity of using a single key for encryption and decryption results in a far more efficient algorithm.

Asymmetric encryption. Asymmetric algorithms utilize key pairs consisting of a public key and private key, rather than relying on a single shared secret key. Both keys of each key pair are generated in such a way that if data is encrypted using the public key, it can only be decrypted by the private key. Knowledge of the public key does not jeopardize the private key, which allows for a single key pair to be generated for all communications, rather than secret keys for each conversation as is required in

symmetric encryption. Examples of asymmetric encryption include RSA, named after Rivest, Shamir, & Adleman (1978), and Pretty Good Privacy (PGP), which was first released by Phil Zimmermann in 1991.

Forward secrecy. While public-key cryptography is highly effective, it is vulnerable to man-in-the-middle attacks. Therefore, in order to satisfy Kerckhoffs (1883) first three principles, one should seek to implement cryptography which affords its users *forward secrecy*, which ensures that prior communications are not vulnerable if a key is compromised in the future. Forward secrecy was first conceptualized by Merkle (1978). However, due to the delay of peer-review, it is actually Diffie & Hellman (1976) who are commonly credited with the first published protocol for forward secrecy. However, in a retrospective introduction to a reprint of Diffie & Hellman's (1976) original paper, Hellman (2002) has since requested that future mention of the protocol be referred to as the Diffie–Hellman–Merkle key exchange, in recognition of Merkle's earlier conceptualization of the public key distribution system.

Tor Anonymity Network

The original purpose of onion routing was only to anonymize the online communication of military intelligence. The Defense Advanced Research Projects Agency (DARPA) also contributed to the development and funding of the research project. Although onion routing was promising in theory, it was easy to recognize the traffic as military communications since all of the nodes participating in circuits belonged to the military. This limitation prevented the military from achieving the desired level of anonymity.

To address this issue, it was decided to publicly release the onion routing protocol in hopes that civilian users would volunteer their devices to participate as nodes in onion routing circuits. Syverson then teamed with MIT researchers Nick Mathewson and Roger Dingledine to develop a useable tool for anonymous communications, which was first released in 2002. Their efforts ultimately led to the creation of the Tor Project, a non-profit organization currently responsible for the management of the Tor Anonymity Network and the Tor Browser Bundle. Tor stands for The Onion Router, but is stylized as simply Tor.

The Tor Anonymity Network relies upon the original onion routing concept and a volunteer network of thousands of users around the world. Each of these volunteers provide access to a device in order for it to be used as a node in the onion routing protocol. Each onion routing circuit consists of three volunteer nodes, with the first and last node referred to as the *guard relay* and *exit relay*, respectively. The transmissions through the Tor circuit are encrypted in layers of AES encryption so that each node can only decrypt its layer, which reveals the IP address for the next node in the circuit (Figure 2.8).

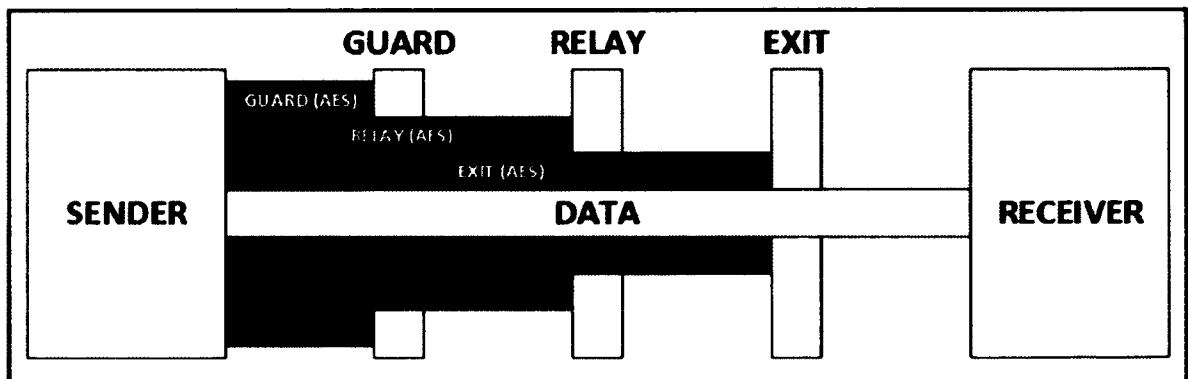


Figure 2.8 – Onion Routing

Communications relying upon the Tor network are routed through randomly generated Tor circuits. These circuits are automatically generated by the Tor client after obtaining a list of available volunteer nodes from a directory server (Figure 2.9). The Tor circuit is then established among all three of the selected nodes (Figure 2.10). After a predefined time interval, or upon visiting a new site, a new circuit is generated (Figure 2.11).

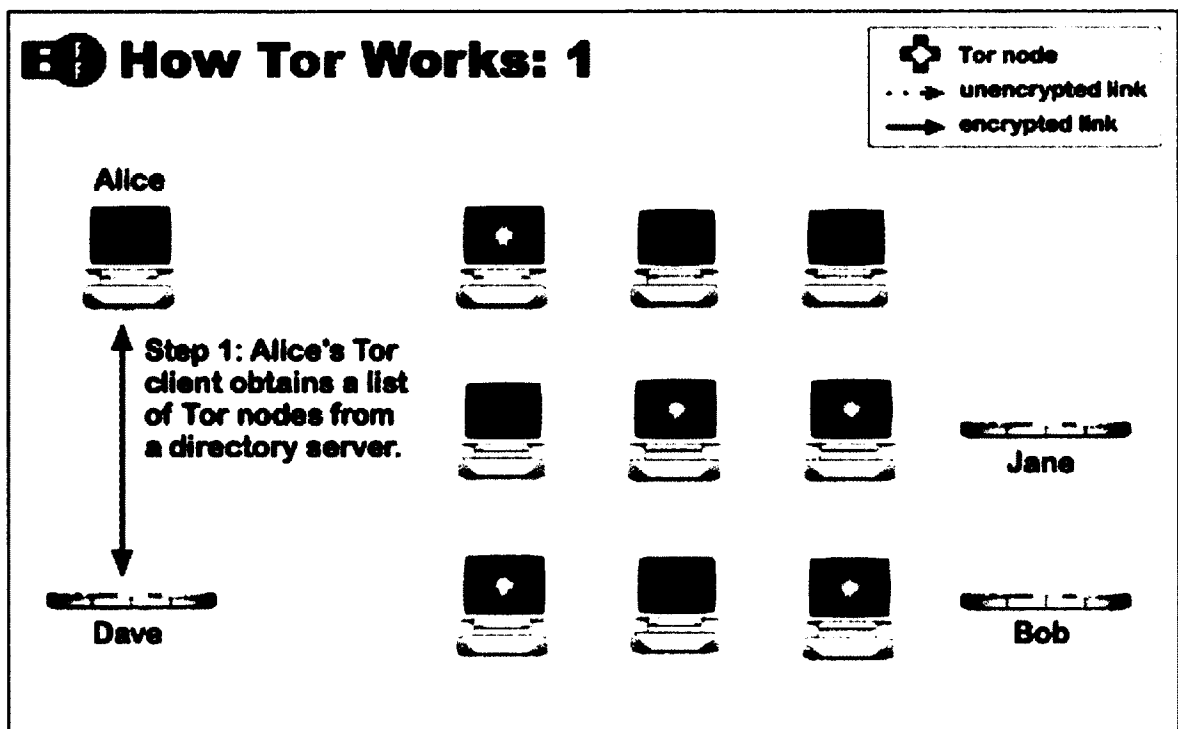


Figure 2.9 – How Tor Works: 1 (The Tor Project, 2015b)

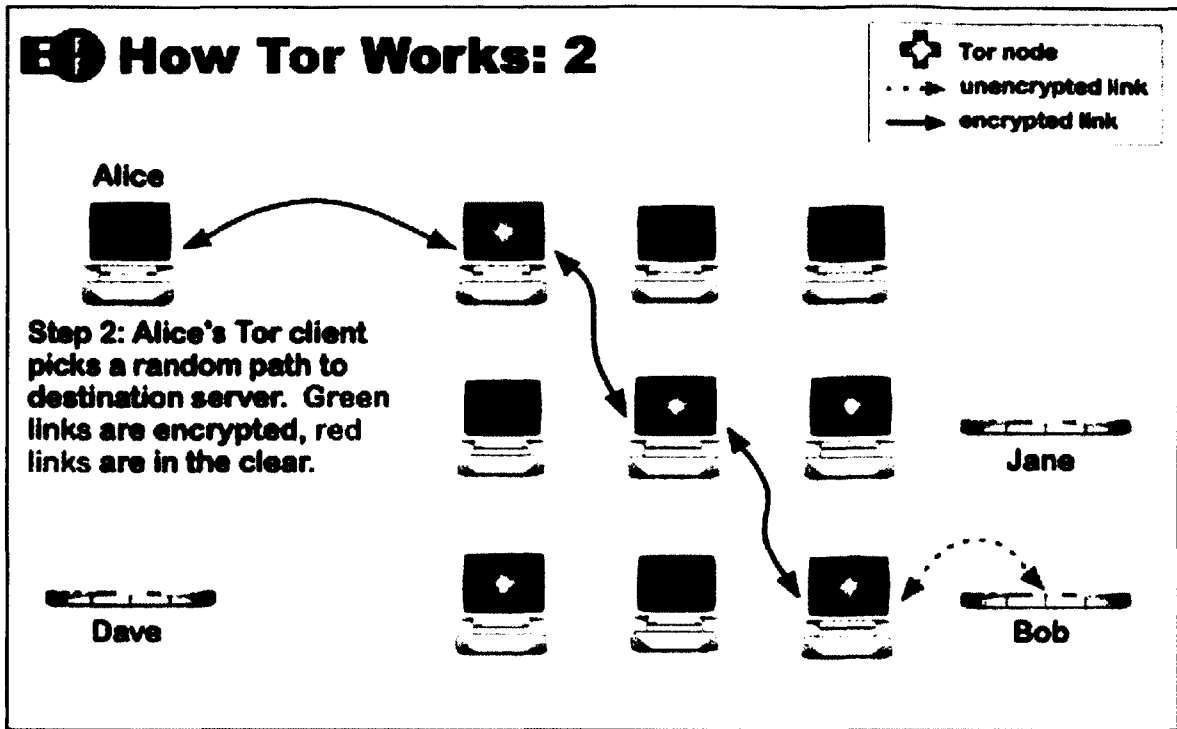


Figure 2.10 – How Tor Works: 2 (The Tor Project, 2015b)

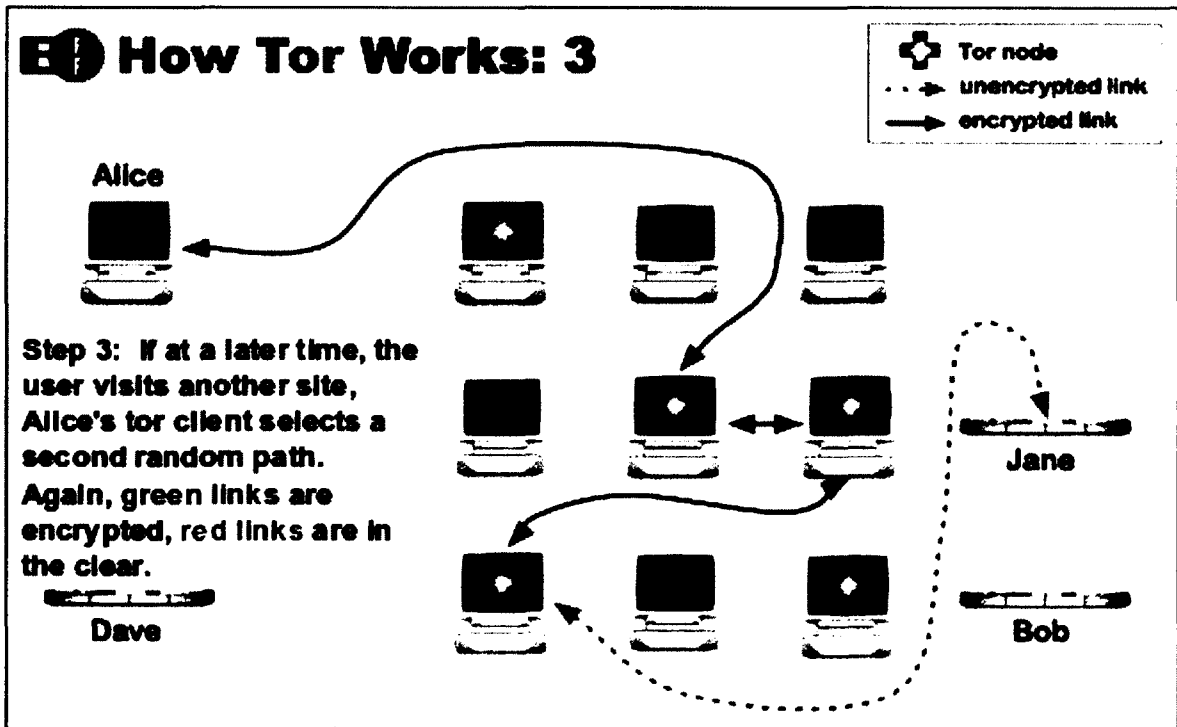


Figure 2.11 – How Tor Works: 3 (The Tor Project, 2015b)

Common attacks. Tor is vulnerable to some known attacks, such as *timing analysis*, *intersection attacks*, *exit node sniffing*. However, none of the vulnerabilities known to date are capable of identifying a specific target user. Instead, these attacks have the potential to reveal the identity of an extremely small subset of users. Therefore, the use of the Tor Anonymity Network provides the greatest level of anonymity protection currently available for common users.

Tor Browser Bundle. In order to provide a user-friendly tool for utilizing the Tor, The Tor Project Based developed the Tor Browser Bundle, which is a modified version of the Mozilla Firefox browser configured to only transmit communications through the Tor Anonymity Network. Although the Tor Browser Bundle does require downloading and familiarizing oneself with a new browser, the similarities with common browsers results in a minimal learning curve. However, due to the additional hops and layers of encryption involved in onion routing, users will experience an increased latency in communications routed through the Tor anonymity network. However, the latency is minimal and should not be noticeable to the user.

Tor Hidden Services. Not only can users protect the IP address of their device, but server administrators can also utilize onion routing to protect the location of their server. This can be achieved through the use of Tor Hidden Services. Servers employing Tor Hidden Services are not accessible by standard web browsers because they do not rely upon the standard Domain Name Server (DNS) for regular websites as it would prevent the anonymization of the IP address. Instead, a randomly generated address for the server is generated and must be provided to users wishing to access it.

While hidden services not being accessible by standard browsers might normally be considered a negative, this is actually a strength for the purposes of the proposed system as it forces users to download the Tor Browser Bundle and therefore prevents users from accidentally revealing their identity. However, this obviously requires that the user familiarize his or herself with the Tor Browser prior to submitting a report. A second strength of utilizing Tor Hidden Services is that it provides full end-to-end encryption by completely encrypting the entire path through two Tor circuits.

In order to establish communication with a Tor Hidden Service, the server must first establish Tor circuits to *introduction points* (IP), which will later be used to establish first contact between visitors and server (Figure 2.12). After the introduction points have been determined, their locations are published in a database for hidden services (Figure 2.13). A user who wishes to access the hidden service then sets up his or her own Tor circuit to a random *rendezvous point*, then looks up the introduction points from the directory and establishes Tor circuits to the IPs (Figure 2.14). The Tor client then asks one of the servers IPs to share the location of the rendezvous point with the server (Figure 2.15). Once the server learns of the location of the rendezvous point, it establishes a Tor circuit (Figure 2.16), completing both circuits between the user and hidden service so that anonymous communication can commence (Figure 2.17).

Tor Hidden Services: 1

Step 1: Bob picks some introduction points and builds circuits to them.

Alice

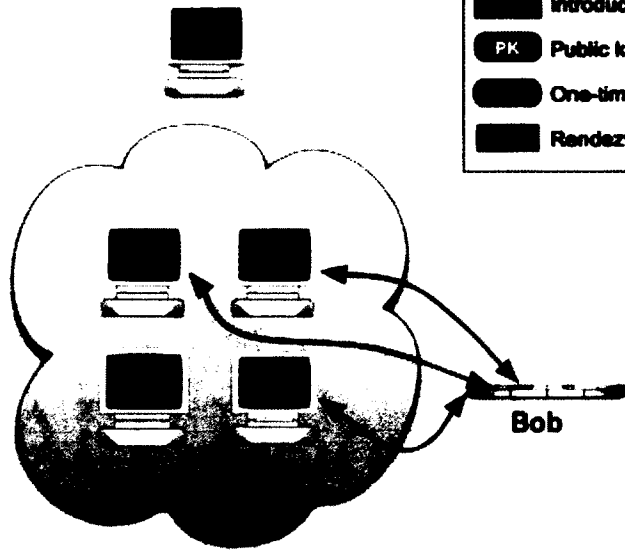


Figure 2.12 – Tor Hidden Services: 1 (The Tor Project, 2015a)

Tor Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.

Alice

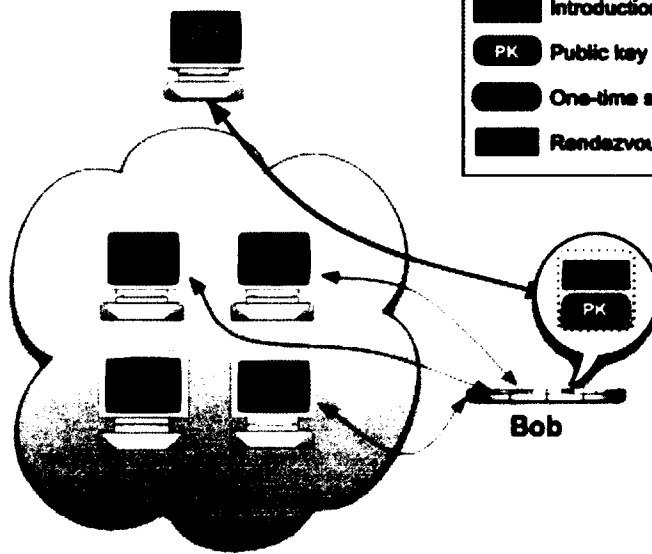


Figure 2.13 – Tor Hidden Services: 2 (The Tor Project, 2015a)

Tor Hidden Services: 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.

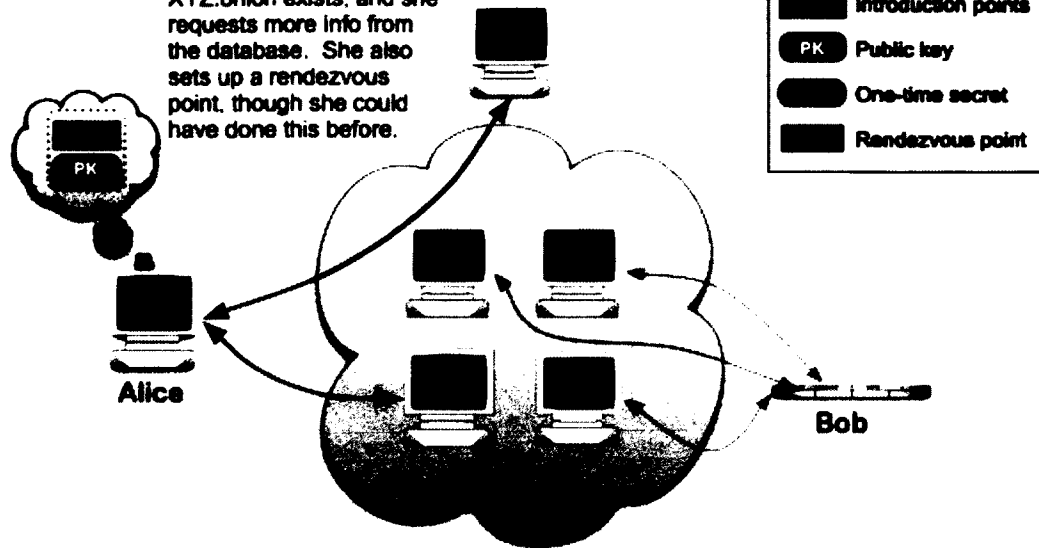


Figure 2.14 – Tor Hidden Services: 3 (The Tor Project, 2015a)

Tor Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.

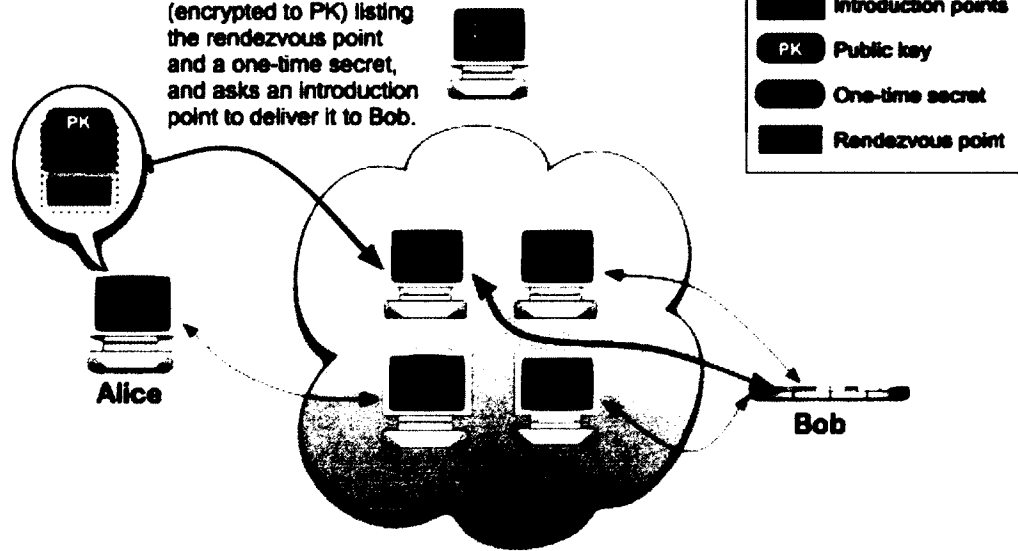


Figure 2.15 – Tor Hidden Services: 4 (The Tor Project, 2015a)

Tor Hidden Services: 5

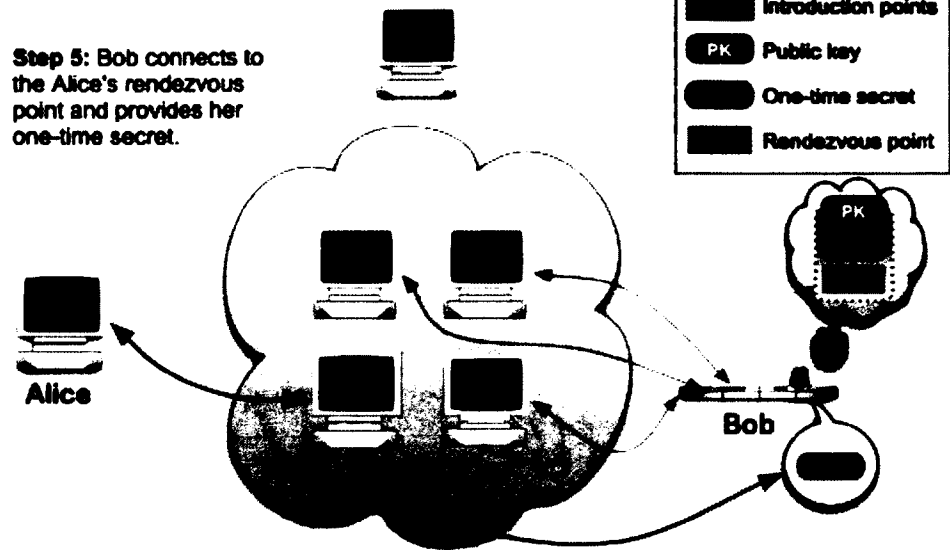


Figure 2.16 – Tor Hidden Services: 5 (The Tor Project, 2015a)

Tor Hidden Services: 6

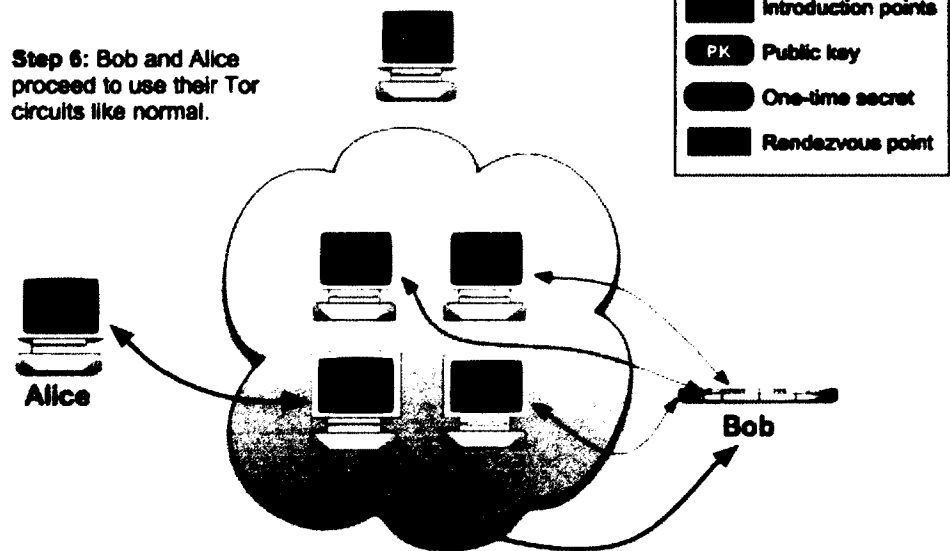


Figure 2.17 – Tor Hidden Services: 6 (The Tor Project, 2015a)

Although Tor provides the strongest anonymity protection currently available via onion routing, a new system called HORNET (High-speed Onion Routing at the Network Layer) has been proposed which aims to provide enhanced performance in terms of speed and scalability (Chen, Asoni, Barrera, Danezis, & Perrig, 2015).

The Amnesic Incognito Live System (Tails)

The Amnesic Incognito Live Systems, commonly known as Tails, is a live operating system designed to employ a number of privacy and anonymity measures, such as encryption and the Tor anonymity network, by default. As a live operating system, Tails can be used independently from a computer's original operating system by booting from a DVD, USB stick, or SD card.

The primary security feature of Tails is that it utilizes the host system's RAM memory, rather than writing to the hard disk drive, in order to have an "amnesic" memory. In doing so, any data stored in the RAM during the session is wiped clean after shutting down Tails. This allows the user to work on sensitive materials without leaving a trace on the host system. Therefore, the use of Tails can benefit both the whistleblower and the investigator by protecting the transmission of sensitive communication and documents prior to and following submission.

Metadata Anonymization

Meta-data is simply data which describe data. Just as academia relies on blind peer-review to ensure fair and objective evaluation of research, anonymous whistleblowers need to be assured that the chosen channel will protect them from the threat of retaliation. Unfortunately, users who have clear and justifiable reasons for remaining anonymous might fail to remove meta-data from supporting documentation,

which might inadvertently reveal their identities. For example, Young (2006) explains how the identity of a peer reviewer was unintentionally revealed to an author due to the meta-data stored in the Microsoft Word document which contained the reviewer's feedback.

While it would be wise for users to scrub any files of all meta-data prior to submission, it would be a disservice to the user not to include additional measures to automatically remove information which has the potential to compromise his or her identity. Therefore, whistleblowers that provide supporting documentation to support their allegations must have protections in place to ensure that such meta-data does not jeopardize their anonymity. There are limited tools currently available to incorporate directly into an online reporting system and it would be best for a custom solution to be developed for this purpose. However, one promising open-source application to consider is the Metadata Anonymisation Toolkit (MAT). MAT is already included in distributions of Tails, but requires the user to remove the metadata from documents prior to submission. Instead, it is suggested that an automatic process for removing metadata from documents be incorporated into the design of the system. A complete description of the program (<https://mat.boum.org/>) and a repository for the MAT source code can be reviewed online (<https://gitweb.torproject.org/user/jvoisin/mat.git>).

User Authentication

Authentication is the process of confirming user identity. Proper user authentication is critical to the security of any sensitive information. Since the publication of the Rainbow Series of U.S. Department of Defense guidelines (National Computer Security Center, 1991), authentication factors have been generally grouped into the

following categories: something users know (*knowledge*), something users have (*ownership*), and something users are (*inherence*). Knowledge factors consist of things the user knows, such as passwords, passphrases, and PINs (personal identification) numbers, as well as information about one's self or family. Possession factors refer to physical objects the user has, such as real and electronic keys, driver's license, and security tokens. Inherence factors, as the name suggest, are inherent to the user and largely consist of biometric characteristics, such as finger prints, facial recognition, and retinal patterns. Since the original categorization, additional factors have emerged: what users do (*active*) and where users are (*location*). Active factors involves dynamic biometrics to capture subconscious behavior, such as typing patterns or walking gait, while location factors ensure that users are in authorized areas prior to granting access, as can be determined with global positioning systems (GPS). The advantages and disadvantages, as well as examples of each factor are outlined in Table 2.14.

Table 2.14 – Advantages and Disadvantages of Authentication Factors

Factor	Examples	Advantages	Disadvantages
Knowledge	Passwords; Personal Identification Numbers (PINs); Passphrases; Personal information	Simple Portable Can be changed as needed Easier to guard than physical objects	Could be forgotten If written down, could be lost, stolen or compromised Easily duplicated by guessing
Ownership	Physical keys; Security tokens; Mobile devices; Identification cards; Security tokens; Radio Frequency Identification (RFID)	More difficult to duplicate Multiple physical objects to use	More difficult to guard than knowledge Requires carrying a physical object Could be lost, stolen or compromised
Inherence	Facial, retinal or iris patterns; Fingerprints; Hand geometry; DNA	Extremely difficult to duplicate Multiple biometric options to use	Specialized equipment required to distinguish characteristics Higher cost Cannot be changed
Active	Typing patterns; Walking gait; Writing patterns and hand pressure	Extremely difficult to duplicate	Specialized equipment required to distinguish characteristics
Location	Physical access controls; Global Positioning System (GPS); Signal triangulation	Difficult to duplicate Must be in an authorized area to access the system	Specialized equipment required to determine location Location can be spoofed Must detect and rescind access when location is no longer satisfied

Multifactor authentication. To achieve the highest degree of security, systems should employ *multifactor* authentication. Multifactor authentication requires the use of one or more types of authentication methods from one or more of the factors, such as coupling a password with a physical security token. Single factor authentication (SFA) only requires the use of one factor, which may even be limited to a single method, such

as a known password. Two-factor authentication (2FA) would require the use of an additional factor, such as the use of a password and fingerprint to access a system.

Accordingly, three-factor authentication (3FA) involves the combination of at least one method from three factors, such as the use of a PIN number, security identification card, and retinal scan.

It is important to reiterate that the use of multiple methods from the same factor does not adequately increase security as each of the methods used would be vulnerable to the same threats. For example, if a purse is stolen, the victim is likely to lose their identification, physical keys and cell phone. All three of these items could be used to authenticate a user through ownership, but they were all compromised simultaneously with a single act of theft. If a system relied upon ownership methods alone, the thief would have very little trouble being authenticated and granted access. Therefore, multifactor authentication (MFA) is desired because the chances of obtaining both secret knowledge and the physical device is far more challenging than obtaining only one of the two. However, anything greater than single factor authentication is not suitable in the context of anonymous whistleblowing as using anything but secret knowledge would require identifying the user from the beginning. Instead, the best option is to ensure that the knowledge factor is as strong as possible, which brings us to a discussion on passwords and passphrases.

Passwords. While there are many types of authentication methods, the most commonly used method for online access is the combination of a username and password, both of which are knowledge factors. Oftentimes a username for authentication purposes is publicly available (e.g., employee email directory), rendering it useless in

terms of secret knowledge. Furthermore, usernames are typically generated and chosen by the user, limiting their anonymity potential. A better approach would be to utilize system generated passphrases.

Passphrases. Although passwords are commonly required to include special characters or at least one capitalized letter, the primary determinant of strength for a given password is actually its length, not the complexity of its characters. It is critical to use passphrases when encrypting data because adversaries can make an unlimited number of attempts to guess the passphrase and are therefore only limited by the resources available. This is explained in the popular XKCD comic provided in Figure 2.18.

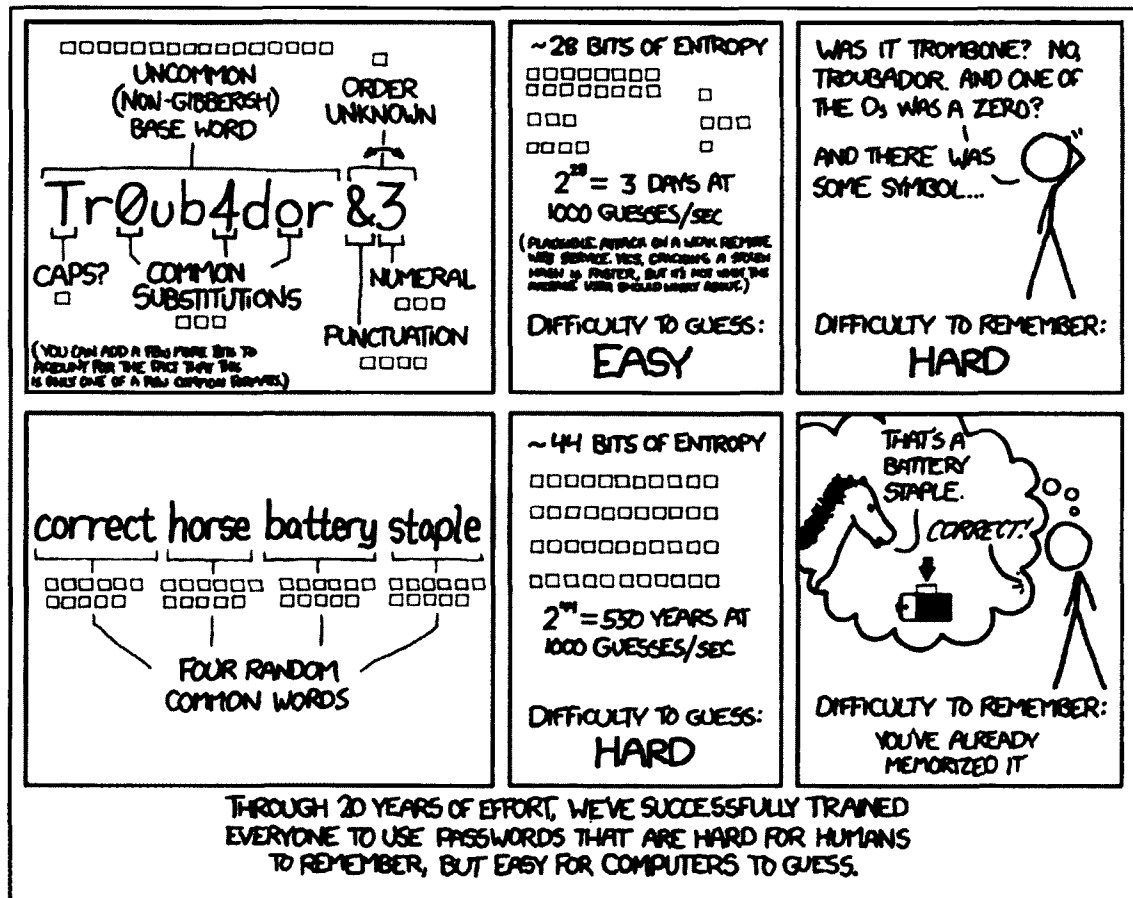


Figure 2.18 – Comic courtesy of XKCD (<https://xkcd.com/936/>)

Authenticating whistleblowers. Upon submission of the initial report, whistleblowers should be provided with a system generated random passphrase. This passphrase will be the only way for the whistleblower to access his or her prior submission. By preventing the user from entering their own passphrase, the system design is able to better protect naive users from utilizing weak or identifiable passphrases. Further, the use of system generated passphrases allows for anonymous, two-way communication, which will be discussed in greater detail in a later section.

Authenticating investigators. Due to the sensitive nature of the information likely to be shared via the system, it is imperative that access only be granted to authorized investigators. Therefore, it is an absolute must for multifactor authentication to be employed prior. This should include physical security controls in addition to standard authentication methods.

Two-Way Anonymous Messaging

Providing users with a randomly generated passphrase upon submission of the initial report allows for the user to reference the case during a subsequent visit to the system. Doing so allows for investigators to leave messages for whistleblowers within the system, which may be used to request clarification of the original submission or additional information. Messages should be automatically deleted after a given time interval in order to prevent the system server from becoming a repository of secrets. The server is already considered a likely target for attackers, but if sensitive information is known to be stored indefinitely, the motivation for attacks will increase.

Investigation Status

In addition to two-way communication, it is highly suggested that standardized stages of investigations be established so that the status of a particular case can be easily communicated to the whistleblower upon follow up. The status can be communicated by simply indicating the stages of the process, as well as a description and expectations for each. This will aid the whistleblower throughout the process of disclosing wrongdoing by keeping them informed of the investigation.

Text-Analysis

While the previous system features have focused primarily on improving the experience for the whistleblower, either in terms of security, anonymity or convenience, the final feature is solely intended to assist investigators. Due to the perception that anonymous sources of information are less credible, investigators must rely upon more objective measures for determining whether alleged wrongdoing is truly credible. One such option for an objective measure of credibility would be through the use of *text analysis*. For example, text analysis has been used to detect deception in written statements (Fuller, Biros, & Delen, 2011; Fuller, Biros, & Wilson, 2009). Incorporating text analysis into the operation of the system would not only allow for written communication from whistleblowers to be analyzed for indicators of deception, but it could also be utilized for assessing credibility itself.

Additional Considerations

Best Practices for Investigators

It is suggested that investigations be conducted by teams with at least three members, rather than assigning reports to individual investigators. This can be enforced via authentication and encryption, which prevents decrypting submissions until all members of the investigation team have provided their authentication signature. Ideally, the authentication for investigators would involve multi-factor authentication, including biometric security measures.

Investigators should also never request that responses be sent or received at a specific time. Instead, a reasonable window of time by which to expect a response should be used. This allows the whistleblower to provide a response at a time he or she perceives to be safest opportunity.

In order to further protect the security and anonymity of users, each message received via the system should be permanently deleted from the system by the investigator after viewing. A record of the information provided in the transmissions can be kept in a secure location elsewhere, but should not be retained within the system to prevent unauthorized access to the case history.

Reporting Metrics

In order to facilitate system and organizational improvement, it is suggested that metrics be calculated to assess performance of the system and organization. For example, according to Penman & O'Mara (2014), NAVEX Global currently calculates a number of reporting benchmarks across all organizations serviced by their EthicsPoint system, such as: types of wrongdoing reported, number of allegations vs. inquiries, report sources

(e.g., groups, locations, business units, departments), levels of employee reporting (e.g., entry-level, middle management), characteristics of anonymous reports, discipline or remediation actions taken, report substantiation rate, report volume, number of retaliation cases and outcomes, and case closure time.

Contributions

This research has provided a number of significant contributions to research and practice. First, this chapter addresses the critical need for the design of an anonymous ethics management system. Second, the proposed system includes the addition of two-way communication capabilities between an anonymous whistleblower and investigator, which has yet to be suggested as a possibility in the whistleblowing literature. This technological advancement has the potential to bridge the perceived credibility gap between anonymous and identified whistleblower reports. Addressing this issue will have tremendous implications for practice in that unethical or illegal behavior reported by anonymous sources will receive greater consideration by investigators. Third, the ability to protect whistleblower anonymity at the system level is the best method for dramatically reducing the incidence of whistleblower retaliation. Fourth, the development of a system that might be preferred over other existing reporting channels by potential whistleblowers would provide organizations with a more effective method of soliciting information regarding unethical or illegal behavior within the organization. An increase in internal reports will provide greater insight into potential problems within the organization, which allows for the appropriate corrective action to be implemented earlier.

Conclusion

The ability for organizations to solicit information on unethical or illegal behavior that would otherwise go unreported provides a significant increase in the ability of the organization to maintain an ethical environment and protect itself from the negative financial, legal and public relations impact such revelations can have on the organization. However, creating an organizational culture that is supportive of whistleblowing and providing an acceptable channel of communication for organizational insiders is challenging due to the sensitive nature of reporting concerns, misconduct and wrongdoing. Therefore, implementing an anonymous ethics management reporting system which utilizes the design to be proposed in this dissertation will allow for improvements in the protection of whistleblowers against retaliation, encourage increased levels of internal reporting, reduce the occurrence of external whistleblowing and provide organizations with the ability to correct unethical or illegal behavior as soon as possible in order to limit the potential damage to the financial, legal and public relations interests of organizations.

CHAPTER THREE

THE IMPACT OF ANONYMOUS, TWO-WAY COMMUNICATION ON PERCEIVED WHISTLEBLOWER CREDIBILITY

Introduction

A widely held and uncontested theory in existing whistleblowing research portends that anonymous reports of wrongdoing are perceived by investigators as less credible than those from identified individuals. However, despite its use in practice, prior whistleblowing research has failed to consider and incorporate two-way communication between whistleblowers and investigators charged with assessing reports of alleged wrongdoing. Thus, this chapter will investigate the impact of two-way communication on this phenomenon, with special attention paid to how investigator perceptions of anonymous reports can be improved using two-way communication by engaging in an asynchronous, computer-mediated dialogue with whistleblowers.

This study reviews existing theories in whistleblowing research and relies upon communication research, both inter-personal and computer-mediated, to address the limitations of prior theory regarding investigator perceptions of anonymous whistleblowers. In order to assess these perceptions, investigators were solicited from a number of professional organizations to participate in an online experiment. The

experiment tasked subjects with evaluating simulated two-way communication between an investigator and an employee attempting to blow the whistle on financial wrongdoing. The theorized relationships and a number of rival explanations were examined in order to account for potential confounds. The empirical results of the study are provided and the implications of the findings are discussed in detail.

Literature Review

Prior to investigating the primary purpose of this study, it is imperative to review the existing research relevant to this phenomenon. This review of the literature begins with basic communication models, continues with computer-mediated communication, and then addresses the role of anonymous communication in the whistleblowing context.

Models of Communication

Shannon's (1948) model of communication, illustrated in Figure 3.1, consists of the following components: information source, transmitter, channel, receiver, destination and noise source. The information source (i.e., sender) produces information to be transmitted. The information is then encoded by a transmitter, transmitted via a channel, and ultimately decoded by the receiver, in order for the destination to interpret the message. However, potential interference in the form of noise may impede transmissions.

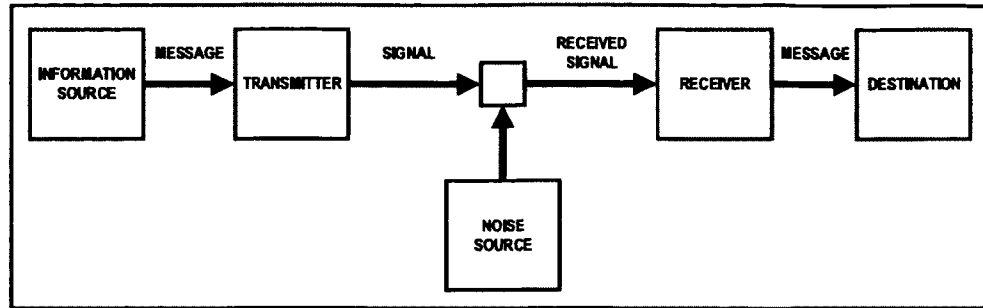


Figure 3.1 – Shannon's (1948) Model of the Communication Process

While Shannon's model is referred to as the first conceptualization of the communication process, it was originally developed for Bell Systems to assist in the development of telephone systems. Therefore, a non-technical model of inter-personal communication was developed by David Berlo (1960) in order to simplify the basic communication process. This model was coined the Sender-Message-Channel-Receiver (SMCR) Model of Communication, and is provided in Figure 3.2.

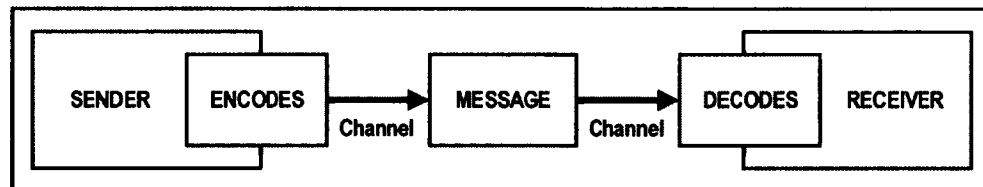


Figure 3.2 – Berlo's (1960) SMCR Model of Communication

However, both models are limited to one-way communication due to the unidirectional nature of such transmissions. Common examples of one-way communication consist of radio and television, as the audience cannot respond to the broadcast. Thus, the inability for the receiver to communicate with the sender in one-way

transmissions may result in a breakdown in communication as the sender cannot verify that the receiver properly received or understood the message.

Barnlund's (1970) addition of feedback to earlier models helps address this issue. This reciprocal, two-way communication method allows for a more thorough exchange of information as the receiver can provide feedback to the sender in order to ask for clarification or confirmation of the original message. An illustration of Berlo's (1960) SMRC Model with the inclusion of Barnlund's (1970) feedback is provided in Figure 3.3. Note that Barnlund (1970) does not explicitly designate a sender or receiver since both parties can dynamically alternate between both roles as many times as necessary.

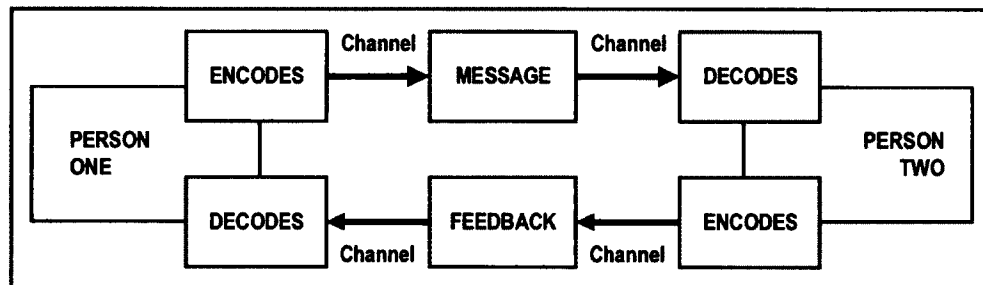


Figure 3.3 – Addition of Barnlund's (1970) Feedback to Berlo's (1960) SMRC Model

The use of feedback also allows the receiver to communicate, both verbally and nonverbally, with the original sender in response to his or her message. For example, facial expressions and body language can provide the sender with nonverbal behavioral cues from the receiver, which informs the sender of communication effectiveness.

Barnlund's (1970) original transactional communication model is illustrated in Figure 3.4.

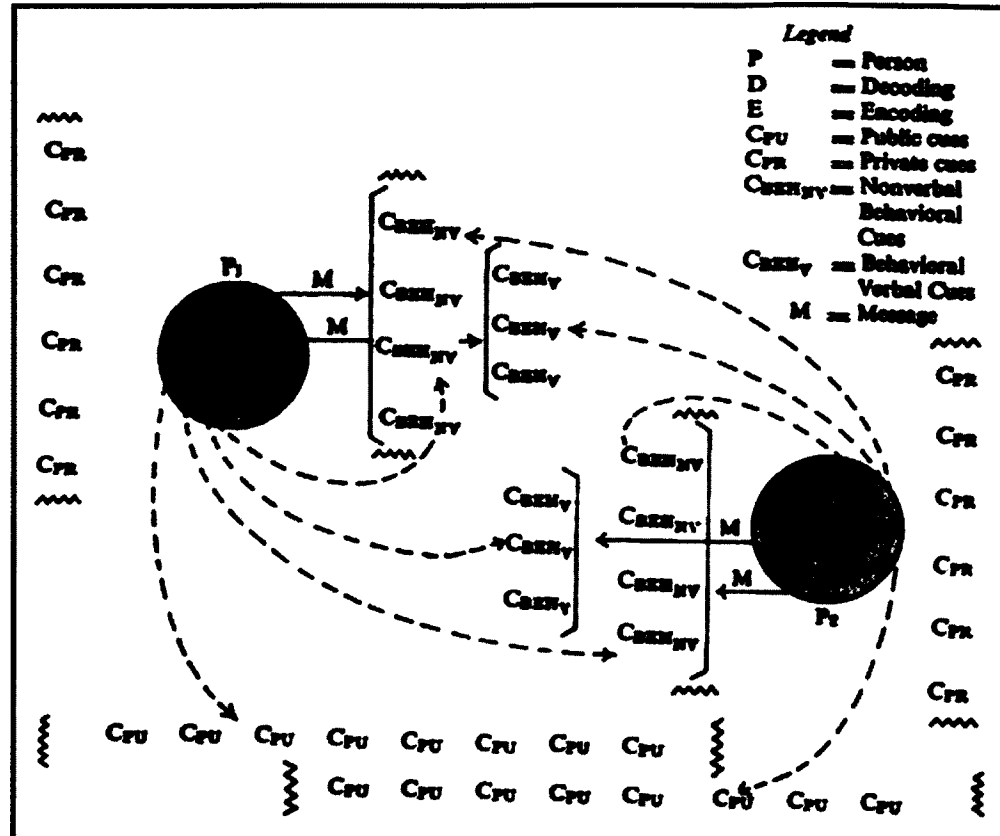



Figure 3.4 – Barnlund's (1970) Transactional Model of Communication

Media Richness Theory

In addition to feedback, it is especially important to note Barnlund's (1970) inclusion of both verbal and nonverbal behavioral cues when assessing the effectiveness of communication. However, such cues are only available if the given medium allows for individuals to transmit and perceive them. Daft & Lengel (1984) classified various communication mediums into a hierarchy of media richness (Table 3.1) based upon common characteristics, such as the celerity of feedback, types of channels and cues, source and language. For example, reports provide only written language, whereas face-to-face conversations allow for the use of oral communication, facial expression, body language and immediate feedback.

Table 3.1 – Daft & Lengel's (1984) Hierarchy of Media Richness

Increasing Media Richness	Media Classification		Media Characteristics			
			Feedback	Channels & Cues	Source	Language
	Face-to-face	Oral	Immediate	Audio & Visual	Personal	Natural
	Telephone	Oral	Fast	Audio	Personal	Natural
	Addressed Documents (e.g. letters, memos)	Written	Slow	Limited Visual	Less Personal	Natural
	Unaddressed Documents (e.g., reports, newsletters)	Written	Slowest	Limited Visual	Impersonal	Numeric or Natural

Media richness theory posits that communication which is conducted via leaner mediums will result in less effective communication due to the reduction in information that can be transmitted within a given time interval (Figure 3.5). For instance, Kalman & Rafaeli (2011) relied upon expectancy theory in order to examine how violations of norms for computer-mediated communication impact perceptions of the relationship between sender and receiver. Specifically, their research found that unexpected pauses in the communication might cause participants to question the intentions of the intended recipient. For example, if a recipient of an email or other asynchronous communication does not acknowledge its receipt or respond within the sender's expected length of time for a response, the sender may begin to question whether the recipient is intentionally ignoring the message. Further, Kalman & Rafaeli (2011) found that the lack of response is likely to increase this perception as more time passes. Common solutions to this

particular issue involve the use of “auto-reply” or “out of the office” messages which can be sent by the email client when the user is unavailable.

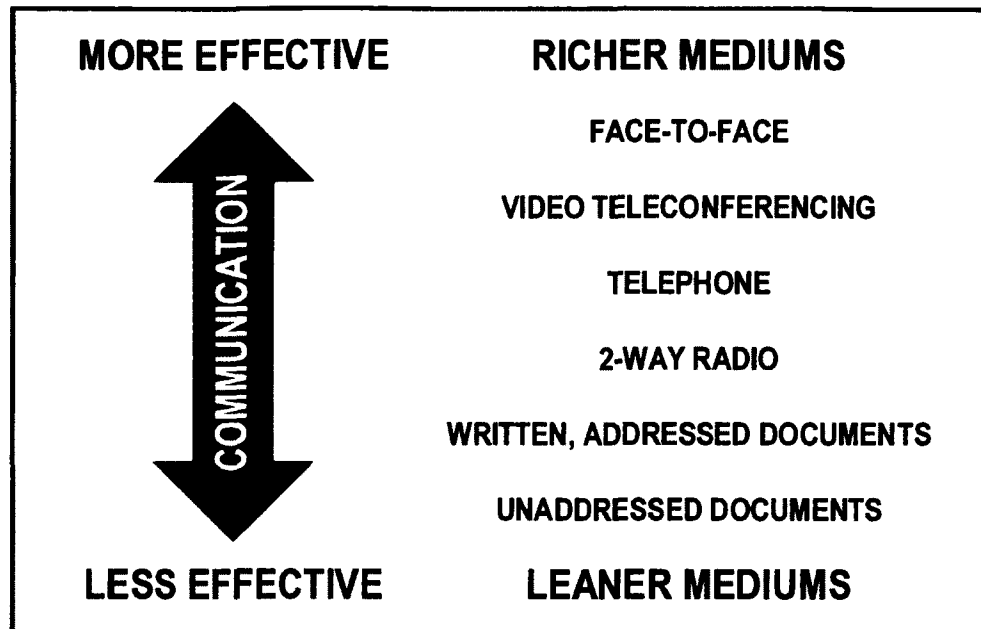


Figure 3.5 – Communication Effectiveness Continuum for Common Mediums

Communication in Whistleblowing

As discussed in Chapter 2, a number of internal and external channels are available for employees to blow the whistle and report wrongdoing. Unfortunately, due to the context of the current research, verbal communication, whether in person or by phone, is not desirable for reporting wrongdoing due to its inability to preserve anonymity. As also explained in Chapter 2, a number of modern technical measures can be implemented in order to allow for anonymous, two-way communication with investigators. With this fact in mind, computer-mediated communication is the best alternative medium for maintaining anonymity without resorting to one-way communication. Therefore, some media richness must be sacrificed for the sake of

preserving anonymity in order to provide whistleblowers with the highest level of protection from potential retaliation.

Role of anonymity. As previously discussed in Chapters 1 and 2, anonymity is of prime importance when concerned with protecting whistleblowers from retaliation. Anonymity measures incorporated into policies, procedures and systems for the reporting of wrongdoing can help alleviate the threat of retaliation. This issue is due to the fact that employees perceive reporting via anonymous channels as less likely to result in employment loss, reputation loss, or harassment (Ayers & Kaplan, 2005; Kaplan & Schultz, 2006, 2007; Near & Miceli, 1995, 1996) and has been shown to result in a more open and thorough exchange of ideas in computer-mediated communication (Jessup & Tansik, 1991).

However, despite all of the advantages for the whistleblower in the reporting of wrongdoing, there are a number of drawbacks which may impede investigations. For example, Near & Miceli (1995, 1996) have long argued that anonymous whistleblowers would be perceived as less credible which may result in less effective investigations. This belief is rooted in the argument made by Elliston (1982) that anyone who is alleged to have committed wrongdoing or misconduct should have the right to confront the individual who alleged the claim. Therefore, if claims are made anonymously, then the accused are unable to fully defend themselves. The reduction in credibility may also occur if the investigator perceives anonymous reports to be ineffective based upon prior experience as investigating anonymous claims are likely to be more time-consuming. Anonymous communications also prevent investigators from assessing the status, integrity, and motives of the individual alleging wrongdoing, which may result in lower

levels of perceived credibility (Near & Miceli, 1995, 1996). Despite the longstanding theories on the subject, no empirical research had been conducted to verify this phenomena.

As previously discussed in Chapters 1 and 2, two-way communication channels are already utilized to report alleged wrongdoing. Therefore, the present study seeks to assess whether the prior theories hold true when whistleblowers and investigators can engage in an active dialogue via anonymous two-way communication.

Hypotheses Development

Based upon the discussion of the literature, one would expect investigators to perceive reports from anonymous sources to be less credible than identified reports. This expectation forms the basis for the first hypothesis of this study.

H1: Investigators will perceive anonymous reports to be less credible when compared to identified reports.

Further, one can expect investigators to gain confidence in the assessment of credibility when provided with the identity of the author of the report. Therefore, the second hypothesis will test this relationship.

H2: Investigators will exhibit more confidence in the assessment of credibility for identified reports as opposed to anonymous reports.

Due to the expected relationships mentioned in H1 and H2, it is anticipated that the perceived credibility gap between anonymous and identified reports will result in a corresponding gap in resource allocation by investigators. Therefore, the third hypothesis will test this relationship.

- H3: Investigators will allocate fewer resources to investigate issues raised in anonymous whistleblower reports when compared to identified reports.

Unfortunately, prior research has neglected to consider the impact of two-way communication on investigator perceptions of credibility. Two-way communication is important because it allows for feedback back to be exchanged, thereby enriching the effectiveness of communication. To test this phenomena, this study will assess how obtaining additional information will improve perceptions of whistleblower credibility and resource allocation for anonymous reports. Therefore, the fourth hypothesis will assess whether investigators who obtain additional information in subsequent communications will reach the same assessment of whistleblowers when compared to those who obtain all information in a single report submission.

- H4a: Investigators who obtain additional substantive information from whistleblowers will perceive whistleblower credibility similarly to those who receive the same amount of information in a single report.
- H4b: Investigators who obtain additional substantive information from whistleblowers will allocate investigatory resources similarly to those who receive the same amount of information in a single report.

Further, when investigators are engaged in two-way communication with a whistleblower, it is possible that the perception of credibility and amount of resources allocated to investigate alleged wrongdoing might be influenced simply by the number of messages rather than any additional substantive information provided. Thus, the fifth hypothesis will assess this potential confound on both credibility and resource allocation.

H5a: Investigators who receive additional communication but are not provided additional information about the reported wrongdoing will perceive higher levels of credibility than those who receive additional communication that provides substantive information.

H5a: Investigators who receive additional communication but are not provided additional information about the reported wrongdoing will allocate fewer investigatory resources than those who receive additional communication that provides substantive information.

Based upon the expectancy violation found in computer-mediated communication when a response is not provided in a timely fashion (Kalman & Rafaeli, 2011), it is hypothesized that investigators will perceive whistleblowers to be less credible if they fail to respond to requests for additional information.

H6: Investigators who do not receive further communication from whistleblowers beyond the initial report will perceive the whistleblower to be less credible than those who receive further communication.

However, it is also theorized that if the whistleblower responds, but is simply unwilling to provide additional information out of concern for his or her well-being due to the threat of retaliation, investigators will understand and recognize this reality without any significant reduction in the perception of whistleblower credibility.

H7: Investigators who receive further communication from whistleblowers, but are provided with no new information will not exhibit a significant reduction in perceived whistleblower credibility when compared to those who receive more information.

Lastly, but most importantly, the efficacy of two-way communication must be shown to achieve equal or better results when compared to one-way communication. Therefore, the final hypothesis of this study will compare perceptions of credibility between those who engage in both one- and two-way communication.

- H8: The credibility of anonymous whistleblowers who engage in two-way communication with investigators will be perceived as equally credible when compared to identified whistleblowers who do not engage in two-way communication.

Methodology

Participants

Compliance officers and accounting professionals served as the primary target populations for this study as they have the necessary education and experience to evaluate reports of financial misconduct. Participants were recruited by soliciting members of a number of professional associations. Compliance professionals were contacted through the Society of Corporate Compliance and Ethics (SCCE). Accounting professionals were recruited from the Association for Certified Fraud Examiners (ACFE), the American Institute of Certified Public Accountants (AICPA) and the Institute of Internal Auditors (IIA). Prior to participating, study subjects were offered the opportunity to have a \$3.00 (USD) donation made on their behalf to a non-profit organization of their choice in exchange for participating in the study.

Experimental Design

A randomized, 2 x 5 between-subjects experimental design was employed in this study. The experiment was conducted online and simulated the communication between an investigator and an employee. The two experimental factors for this study consist of anonymity (i.e., anonymous or identified) and five levels of simulated communication, each of which manipulate the number of messages provided by the whistleblower and the amount of information contained within each.

Procedure

Participants were asked to read and review background information (Figure 3.6) which tasked them with assuming the role of an outside compliance consultant by a fictitious company, Vitrum Technologies, Inc. In this position, participants would be responsible for reviewing a whistleblowing communication exchange between an employee and investigator via an internal reporting system.

Please read the following background information before proceeding to the next page.

You have recently been hired by Vitrum Technologies, Inc. to serve as an outside compliance consultant. Vitrum is a U.S.-based, publicly-traded company that develops, manufactures, and markets high-performance film-coated glass used in such products as computer screens, photocopiers, and projection televisions. The company was incorporated in 1994, and from its inception through 1997 was primarily engaged in the development of process and product technology, with limited commercial production.

The company has successfully developed a unique, proprietary process for applying thin film coatings to glass and other products that it believes represents a fundamental technological breakthrough. However, since the implementation of this technology in early 1998 they have not captured a significant share of the market for this type of process, and the majority of their sales have been to two principal customers.

Vitrum's common stock was initially registered with the SEC in May 2000, and is quoted on the NASDAQ. Vitrum has been audited by the same Big 4 accounting firm for the preceding five years. Vitrum's auditor has always issued standard, unqualified (i.e. clean) audit reports. Following the requirements established by the Sarbanes–Oxley Act of 2002, Vitrum implemented an online system that allows employees to report any potential problems directly to compliance officers and the internal audit committee through reporting channels capable of anonymous, two-way communication.

Your role as an outside compliance consultant is to review the internal compliance controls currently in place at Vitrum. Specifically, you will review and assess a report of alleged wrongdoing submitted through the Vitrum Reporting System in January 2015. At this time the company was preparing for an audit of their annual financial statements for the year ended December 31, 2014, which were to be included in their Form 10K filed with the SEC. After reviewing the information contained in the report, you are responsible for (1) assessing the credibility of the report and (2) determining the amount of resources to be allocated to investigate the alleged wrongdoing.

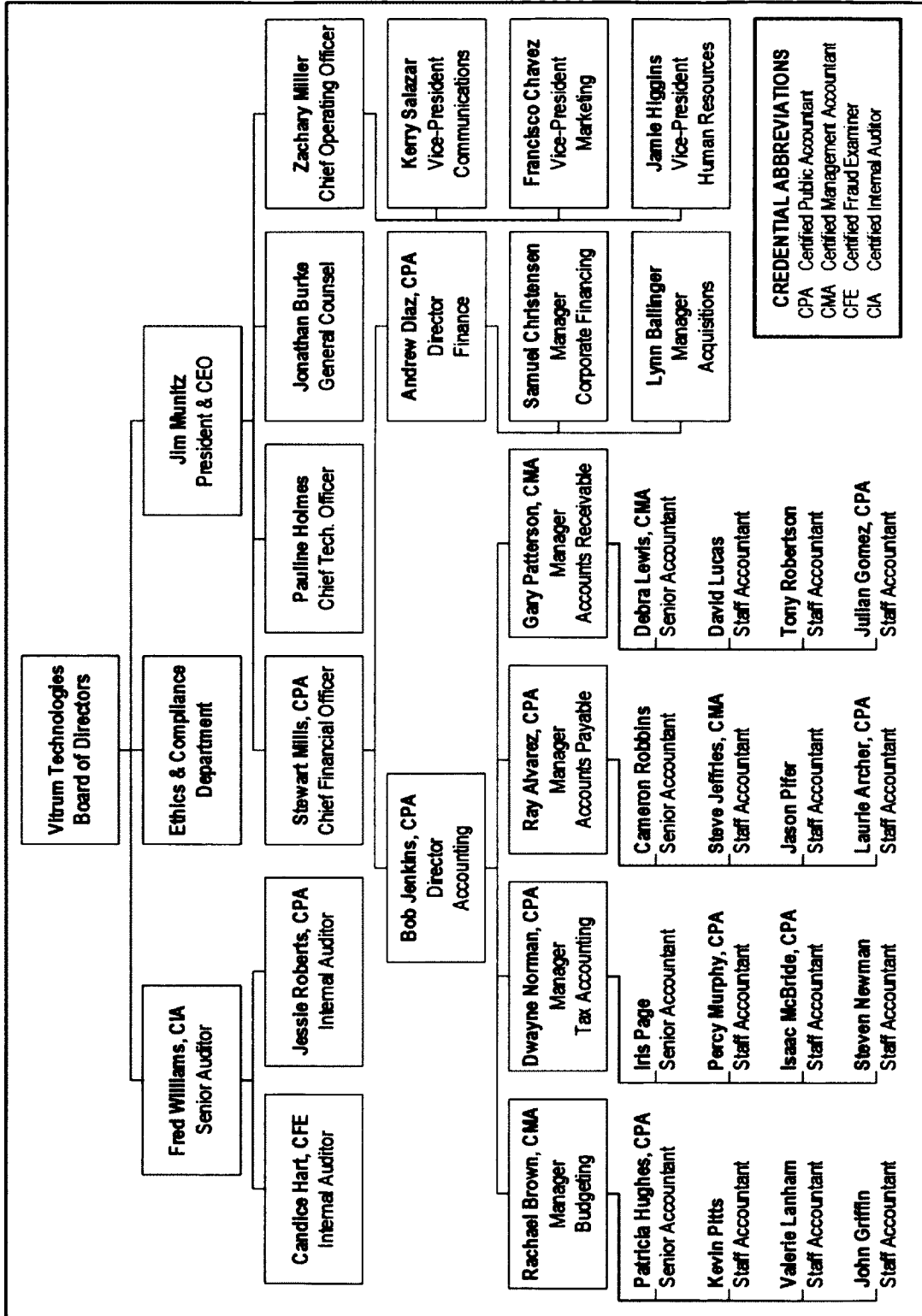
Before proceeding to the next step, please open the following links in new browser tabs or windows so that you may reference them throughout the rest of the study. The first link contains information regarding Vitrum's financial situation for the previous three years. The second link provides an organizational chart of Vitrum's top management and their direct subordinates. Should you accidentally close either link, they may be accessed again at the top of the following pages.

Figure 3.6 – Background Information

Supplemental financial data for the preceding three years (Figure 3.7) and an organizational chart was also provided to the participants (Figure 3.8) in order to provide context to the organizational structure and financial standing of the company at the time the report was received.

Vitrum Technologies, Inc.			
Period Ending	Dec. 31, 2012	Dec. 31, 2013	Dec. 31, 2014 (unaudited)
Balance Sheet:			
Current assets	\$1,569,010	8,374,559	6,068,392
Property and equipment	5,779,044	8,394,457	23,235,573
Other assets	31,782	262,170	
	\$7,379,836	17,031,186	29,303,965
Current liabilities	\$2,936,994	12,234,619	6,081,206
Long term liabilities	633,691	915,340	793,376
Common stock	7,993,400	8,005,460	29,191,905
Retained earnings (deficit)	(4,184,249)	(4,124,233)	(6,762,522)
	\$7,379,836	17,031,186	29,303,965
Income Statement:			
Revenue	\$1,097,683	4,035,382	8,063,848
Cost of sales	1,219,954	2,458,226	6,232,346
Gross (loss) profit	(122,271)	1,577,156	1,831,502
Operating expenses	1,489,084	1,173,424	4,375,750
Interest expense	74,688	343,716	94,041
Net (loss) income	(\$1,686,043)	60,016	(2,638,289)

Figure 3.7 – Financial Reports for Vitrum Technologies, Inc.



CREDENTIAL ABBREVIATIONS
 CPA Certified Public Accountant
 CMA Certified Management Accountant
 CFE Certified Fraud Examiner
 CIA Certified Internal Auditor

Figure 3.8 – Organizational Chart for Vitrum Technologies, Inc.

A scenario employed by Shafer (2002) was adapted into simulated

communication from an employee wishing to report financial misconduct. Each treatment was provided with a transcript of communication, initiated by either an anonymous or identified source, which alleges financial wrongdoing. Communication with the employee was simulated using five different levels, which varied in the amount of information provided in the initial report [full vs. half], as well as manipulated whether the simulated whistleblower provides additional information [i.e., the remaining half], responds but is unwilling to provide additional information, or does not respond at all. Levels 1 and 5 did not have a third round of communication due to the fact that no response was provided in round B. The treatment matrix can be seen in Table 3.2, and the simulated messages used for each treatment are provided in Table 3.3.

Table 3.2 – Experimental Treatments

Level	Round A	Round B	Round C
1	Full Info	No Response	N/A
2	Full Info	No New Info	No Response
3	Half Info	Half Info	No New Info
4	Half Info	No New Info	No Response
5	Half Info	No Response	N/A

Table 3.3 – Simulated Communication from Whistleblower

	ROUND A	ROUND B	ROUND C
1	<p>[My name is Bob Jenkins and] I have been a Certified Public Accountant for Vitrum for the past year and a half. Due to the company's poor results and the failure to meet market forecasts, our CEO, Jim Munitz, approached me about a plan to backdate sales invoices and shipping documents for a large number of sales made during the first quarter of next year so that the sales could be recognized in 2014. He said one of Vitrum's freight carriers has agreed to backdate their bills of lading to correspond with the company's shipping documents. Jim has now asked me to accelerate the recognition of approximately \$2,000,000 in revenue for the first quarter of 2015. This plan would increase gross profit and reduce the reported net loss in 2014 by approximately \$1,000,000. Please look into this as soon as you can because we need to prepare the financial statements and I am really concerned about losing my job if I don't comply with the CEO's request.</p>	<p>No response.</p>	<p>N/A</p>
2		<p>Unfortunately, I have provided all that I am willing to disclose at this time.</p>	<p>No response.</p>
3	<p>[My name is Bob Jenkins and] I have been a Certified Public Accountant for Vitrum for the past year and a half. Due to the company's poor results and the failure to meet market forecasts, our CEO, Jim Munitz, approached me about a plan to backdate sales invoices and shipping documents for a large number of sales made during the first quarter of next year so that the sales could be recognized in 2014. Please look into this as soon as you can because we need to prepare the financial statements and I am really concerned about losing my job if I don't comply with the CEO's request.</p>	<p>Yes. In fact, Jim just told me that one of Vitrum's freight carriers has agreed to backdate their bills of lading to correspond with the company's shipping documents. Jim has now asked me to accelerate the recognition of approximately \$2,000,000 in revenue for the first quarter of 2015. This plan would increase gross profit and reduce the reported net loss in 2014 by approximately \$1,000,000. Again, please investigate this as soon as possible because we need to prepare the financial statements and I am really concerned about losing my job if I don't comply with the Jim's request.</p>	<p>Unfortunately, I have provided all that I am willing to disclose.</p>
4		<p>Unfortunately, I have provided all that I am willing to disclose at this time.</p>	<p>No response.</p>
5		<p>No response.</p>	<p>N/A</p>

A reply from the investigator was provided for each message from the employee. After round A, the investigator requested additional information to assist in the investigation. If more information was received in a second message, the investigator thanked the employee for the additional response and also included assurances that their identity would remain either confidential or anonymous, dependent upon the treatment. A screenshot of the simulated communication, as seen by participants assigned to identified treatment number 2 (I2), is provided in Figure 3.9. In addition to providing participants with a transcript, custom Cascading Style Sheets (CSS) were applied in order to stylize the look of the reporting system interface in Qualtrics for a more realistic experience.

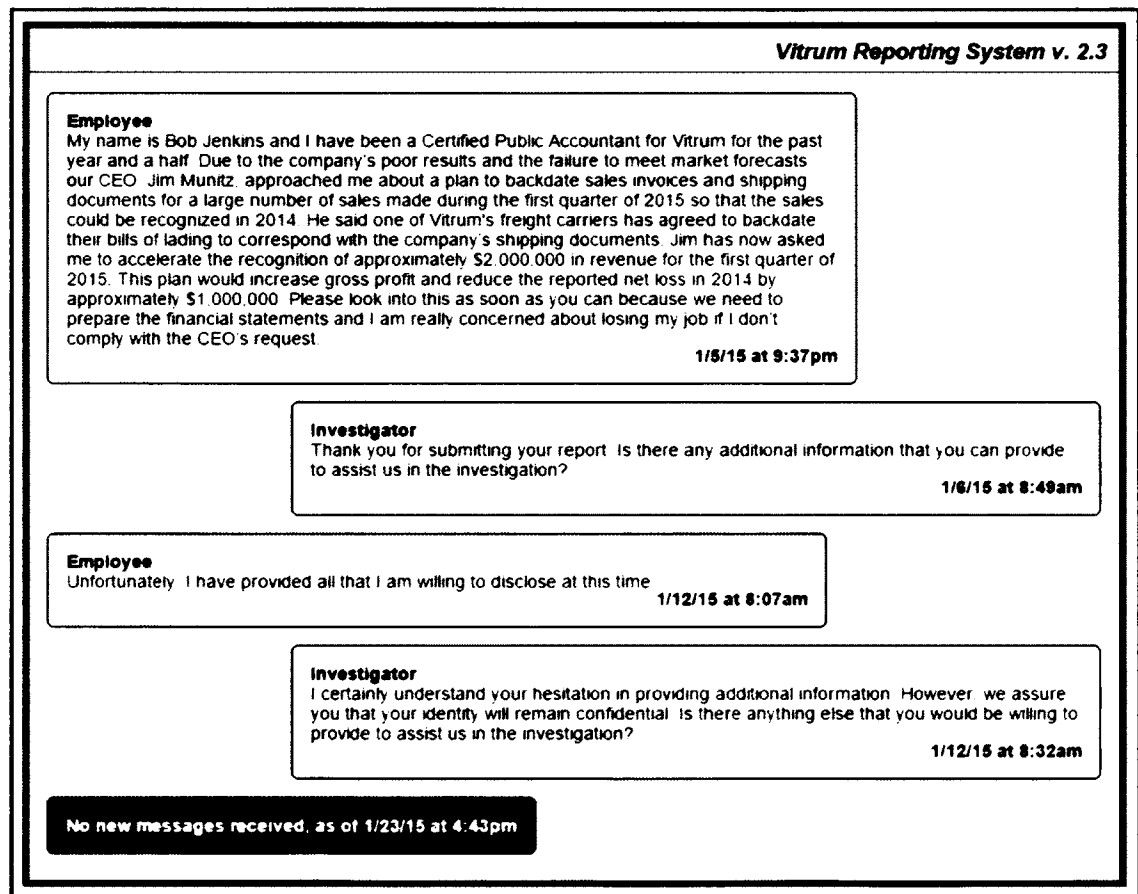


Figure 3.9 – Screenshot of Simulated Communication

After reading the exchange of communication between employee and investigator, participants were asked to rate the credibility of each report, indicate their level of confidence in the assessment of credibility, and allocate an appropriate level of resources to investigate the issue alleged in the report. Credibility and confidence in the assessment of credibility were assessed on a scale from 0 to 100, while investigatory resources was measured from \$0 to \$100,000. To ensure that participants considered an adequate trade-off when allocating resources, the original thought was to suggest that the \$100,000 funds remaining in the monthly budget for investigations were needed for a new product-line with excellent profit-generating potential. However, considering that the sample of this study consists of those who are charged with investigating reports of wrongdoing, the inclusion of a product-line may not generate an appropriate trade-off. Therefore, the phrasing of the question, provided in Figure 3.10, was instead altered to a time-sensitive need for the implementation of a new compliance program.

Recall, the initial report was received on January 5, 2015. When budgeting for potential investigations that may result from reports, the board of directors assumed that there could be as many as two reports per month and that each investigation would cost approximately \$50,000, resulting in a total monthly budget of \$100,000.

Assume that you still have \$100,000 remaining in the board's January 2015 budget and that no other reports would be investigated that month. Therefore, any funds that you do not use to investigate this report will carry forward to the February 2015 budget, in which there is a dire need for another \$100,000 to implement a new compliance program, which has been mandated by the board of directors and must be implemented by February 28, 2015.

Based upon the information provided in the report, use the slider below to indicate the dollar amount of the January 2015 investigation budget that you would have allocated toward investigating the alleged wrongdoing.

Figure 3.10 – Resource Allocation Measure

Manipulation Checks

Prior to evaluating the communication between the employee and investigator, participants answered a number of questions designed to assess the effectiveness of each manipulation and ensure the validity of the experimental design. Each of the five manipulation checks were significant, as can be seen in Table 3.4.

Table 3.4 – ANOVA Results for Manipulation Checks

Dependent Variable	Source	Sum of Squares	Df	Mean Square	F	Sig.
How many messages were sent by the source of the report? ¹	Between Groups	65.59	9	7.29	25.43	.000***
	Within Groups	85.12	297	.29		
	Total	150.71	306			
Did the employee provide his or her name? ²	Between Groups	71.25	9	7.92	411.29	.000***
	Within Groups	5.74	298	.02		
	Total	76.99	307			
How would you rate the source of the report? ³ Anonymous : Identified	Between Groups	478.37	9	53.15	34.95	.000***
	Within Groups	453.18	298	1.52		
	Total	931.54	307			
Did investigator promise identity would remain confidential? ²	Between Groups	46.85	9	5.21	80.67	.000***
	Within Groups	19.23	298	.07		
	Total	66.08	307			
Did investigator promise identity would remain anonymous? ²	Between Groups	57.44	9	6.38	142.06	.000***
	Within Groups	13.30	296	.05		
	Total	70.74	305			

NOTE: *** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$

¹ This item was measured using a text box.

² This item was measured using a “Yes” or “No” question.

³ This item was measured using a 7-point Likert scale from “Fully Anonymous” to “Fully Identified.”

Results

Sample Demographics

The total usable sample of 301 respondents consisted of 65% males (Table 3.5), with an average age of 49 years, ranging from 20 to 84 years old (Table 3.6). Over 94% have attained at least a bachelor's degree (Table 3.7). Organizational tenure, organization type and industry demographics for the sample are provided in Table 3.8, Table 3.9, and Table 3.10, respectively.

Table 3.5 – Sample Gender

Gender	Frequency	Percent
Males	196	65.1
Females	94	31.2
Missing	11	3.6
Total	301	100.0

Table 3.6 – Sample Age

Age (in years)	Frequency	Percent	Cumulative Percent
< 20	0	0.0	0.0
20 – 29	14	4.7	4.7
30 – 39	64	21.3	25.9
40 – 49	57	18.9	44.9
50 – 59	85	28.2	73.1
60 – 69	52	17.3	90.4
> 70	12	4.0	94.4
Missing	17	5.6	100.0
Total	301	100.0	

Table 3.7 – Sample Education Level

Type	Frequency	Percent	Cumulative Percent
High School / GED	2	0.7	0.7
Some College	5	1.7	2.3
Associate's Degree	114	37.9	40.2
Bachelor's Degree	139	46.2	86.4
Master's Degree	13	4.3	90.7
Doctoral Degree	18	6.0	96.7
Professional Degree (JD, MD)	10	3.3	100.0
Missing	0	0.0	100.0
Total	301	100.0	

Table 3.8 – Organizational Tenure

Tenure (in years)	Frequency	Percent	Cumulative Percent
0 – 1	31	10.3	10.3
2 – 3	43	14.3	24.6
4 – 5	45	15.0	39.5
6 – 7	26	8.6	48.2
8 – 9	20	6.6	54.8
10 – 11	26	8.6	63.5
12 – 13	14	4.7	68.1
14 – 15	16	5.3	73.4
16 – 17	11	3.7	77.1
18 – 19	9	3.0	80.1
20 – 21	10	3.3	83.4
22 – 23	7	2.3	85.7
24 – 25	7	2.3	88.0
> 25	21	7.0	95.0
Missing	15	5.0	100.0
Total	301	100.0	

Table 3.9 – Type of Organization

Type	Frequency	Percent	Cumulative Percent
Private, For-Profit	139	46.2	46.2
Private, Not-For-Profit	28	9.3	55.5
Public, For-Profit	11	3.7	59.1
Public, Not-For-Profit	14	4.7	63.8
Local Government	5	1.7	65.4
State Government	15	5.0	70.4
Federal Government	29	9.6	80.1
Self-Employed	1	0.3	80.4
Missing	59	19.6	100.0
Total	301	100.0	

Table 3.10 – Industries Represented

Industry	Frequency	Percent	Cumulative Percent
Accounting	98	32.6	32.6
Banking	5	1.7	34.2
Chemical	1	0.3	34.6
Consulting	36	12.0	46.5
Consumer Products	1	0.3	46.8
Defense	2	0.7	47.5
Education	19	6.3	53.8
Energy	6	2.0	55.8
Entertainment & Leisure	2	0.7	56.5
Financial Services	31	10.3	66.8
Health Care	30	10.0	76.7
Legal	8	2.7	79.4
Manufacturing	11	3.7	83.1
Pharmaceuticals	1	0.3	83.4
Real Estate	1	0.3	83.7
Retail & Wholesale	6	2.0	85.7
Service	11	3.7	89.4
Software	3	1.0	90.4
Sports	2	0.7	91.0
Technology	8	2.7	93.7
Telecommunications	1	0.3	94.0
Transportation	3	1.0	95.0
Missing	15	5.0	100.0
Total	301	100.0	

Hypotheses Tests

Descriptive statistics for each of the 10 treatment groups is provided in Table 3.11, with an average treatment size of 30 participants. Prior to testing the planned comparisons for each of the hypothesized relationships, Analysis of Variance (ANOVA) was used to test main effects for each of the three primary variables, credibility, and confidence in credibility and investigatory resources. The results, provided in Table 3.12, indicate that report credibility and confidence in the credibility assessment do vary among the treatment groups, but investigatory resources do not.

Table 3.11 – Descriptive Statistics for Treatment Groups

Group	Experimental Factors			Group Size	Credibility		Confidence		Resources	
	Anon.	Content	Messages		Mean	S. D.	Mean	S. D.	Mean	S. D.
A1	Yes	Full	1	27	72.74	15.13	65.37	20.93	62.74	27.77
A2	Yes	Full	2	32	78.50	14.19	80.81	15.68	69.09	26.50
A3	Yes	Full	3	34	73.79	14.43	76.06	20.33	54.68	30.40
A4	Yes	Half	2	33	71.85	17.17	72.70	24.12	58.85	28.47
A5	Yes	Half	1	27	64.67	20.67	66.74	25.57	56.78	25.31
I1	No	Full	1	32	78.31	17.75	80.47	17.17	63.84	26.65
I2	No	Full	2	30	77.50	14.93	73.17	19.28	62.43	29.73
I3	No	Full	3	29	80.97	15.82	79.86	16.31	63.34	29.25
I4	No	Half	2	30	76.87	18.32	76.27	17.08	57.60	28.78
I5	No	Half	1	27	80.52	14.49	77.11	19.76	57.15	29.54
Totals				301	75.62	16.75	75.06	20.15	60.67	28.20

Table 3.12 – ANOVA Results for Main Effects

Dependent Variable	Source	Sum of Squares	df	Mean Square	F	Sig.
Credibility	Between Groups	6,172.53	9	685.84	2.56	.008***
	Within Groups	78,034.53	291	268.16		
	Total	84,207.06	300			
Confidence in Credibility	Between Groups	7,550.48	9	838.94	2.14	.027**
	Within Groups	114,249.33	291	392.61		
	Total	121,799.80	300			
Investigation Resources	Between Groups	5,367.09	9	596.34	.74	.668
	Within Groups	233,223.00	291	801.45		
	Total	238,590.09	300			

NOTE: *** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$

The assumption of homogeneity of variance was assessed using Levene's (1960) test for each of the dependent variables under examination. The results, provided in Table 3.13, indicate that homogeneity of variance can be assumed for both Credibility and Investigation Resources, but cannot be assumed for Confidence in Credibility.

Table 3.13 – Tests of Homogeneity of Variance

Dependent Variable	Levene Statistic	df1	df2	Sig.
Credibility	1.569	9	291	.124
Confidence in Credibility	2.027	9	291	.036**
Investigation Resources	.444	9	291	.911

NOTE: *** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$

In order to assess the hypothesized relationships, six planned comparisons were constructed according to the contrast coefficients provided in Table 3.14. The first

contrast compares anonymous treatments with identified treatments. The second contrast compares treatment groups that received additional information in a subsequent message (A3 & I3) with those that only received a single message which contained full information (A1, A2, I1, & I2). Contrast number three compares treatments that provided full information (A1, A2, I1, & I2) with those that only provided half (A4, A5, I4, & I5). The fourth contrast is used to compare the treatments with a single message from the whistleblower (A1, A5, I1, & I5) to those that received multiple messages (A2, A3, A4, I2, I3, & I4). Contrast number five was used to assess the difference between treatments which received additional information (A3 & I3) with treatments which received a response, but did not provide additional information (A2, A4, I2, & I4). The sixth and final comparison was conducted in order to compare the credibility of an anonymous treatment which exhibited two-way communication with full information (A3) to that of identified treatments which were only with provided a single message (I1 & I5).

Table 3.14 – Planned Comparisons Contrast Coefficients

Contrast	Treatment Group									
	A1	A2	A3	A4	A5	I1	I2	I3	I4	I5
1	1	1	1	1	1	-1	-1	-1	-1	-1
2	1	1	-2	0	0	1	1	-2	0	0
3	1	1	0	-1	-1	1	1	0	-1	-1
4	3	-2	-2	-2	3	3	-2	-2	-2	3
5	0	-1	2	-1	0	0	-1	2	-1	0
6	0	0	2	0	0	-1	0	0	0	-1

An ANOVA test was then conducted for each contrast to test the hypothesized relationships for the study. The results of the planned comparisons are provided in Table

3.15. The first hypothesis was tested by comparing the assessment of report credibility for anonymous treatments against the credibility for identified treatments. Consistent with prior theory, the results for this hypothesis support the theorized relationship as the anonymous group resulted in a mean credibility rating over 32 percentage points lower than the identified treatments.

Table 3.15 – ANOVA Results for Planned Comparisons

Hypothesis	Contrast	Measure	Difference	Std. Error	t Statistic	df	Sig.
H1	1	Credibility	-32.61	9.471	-3.44	291	.001***
H2	1	Confidence	-25.20	11.459	-2.20	291	.015**
H3	1	Resources	-2.23	16.373	-.14	291	.892
H4a	2	Credibility	-2.47	10.206	-.24	291	.809
H4b	2	Resources	22.07	17.644	1.25	291	.212
H5a	3	Credibility	13.15	8.518	1.54	291	.062*
H5b	3	Resources	27.74	14.726	1.88	291	.031**
H6	4	Credibility	-30.23	23.445	-1.29	291	.099*
H7	5	Credibility	4.80	10.145	.47	291	.636
H8	6	Credibility	-11.24	7.061	-1.59	291	.112

NOTE: *** p < 0.01; ** p < 0.05; * p < 0.10; **One-tailed Tests:** H1, H2, H3, H4b, H5b, H6

The results of the test for hypothesis two also indicated significant support for the theorized relationship that investigator confidence in the assessment of credibility is impacted by whether the source of the report is anonymous or identified. This test revealed a 25 percentage point reduction in the confidence rating. Despite the violation of the assumption of homogeneity of variances for Confidence in Credibility, the results of significance testing for hypothesis two showed that a violation of this assumption does not impact the tests for Confidence in Credibility as the significance level of .015 was the same, regardless of whether equal variances were assumed. Like the previous hypotheses,

hypothesis three was also assessed with contrast number one. The results of this study indicate that there are no differences between the amount allocated to investigate anonymous and identified reports. While this finding is contrary to prior theory, rival explanations can be formulated to account for this unexpected result. First, since the study did not manipulate the alleged wrongdoing under examination, it is possible that all investigators felt that the situation was worth investigating for the same amount, irrespective of their opinions of credibility. It is also possible that due to the nature of anonymous reporting, investigators felt that it would require more, not fewer, resources to investigate the alleged wrongdoing. If so, any potential gap in resource allocation that may have existed otherwise might have been eliminated due to the increase in resources necessary to investigate a more challenging report.

The fourth hypothesis theorized that additional information would allow investigators to reach the same opinion of the alleged wrongdoing as those who received all of the information in a single message. Thus, this hypothesis was assessed in two parts in order to test the effect on both assessment of credibility and the allocation of resources. First, H4a employed contrast number two to compare treatments with full information in a single report to that of treatments which obtained full information across multiple messages. Second, H4b tested the same relationship on the allocation of investigatory resources. The insignificant differences between means for both tests support the theory that two-way communication allows investigators to reach the same conclusion if additional information is obtained.

The test for hypothesis five was also conducted in two parts and employed contrast number three in order to test the possibility of perceptions of credibility and

resource allocation simply being the result of exchanging multiple messages, irrespective of the whether any substantive information was gained. This hypothesis was supported as the expected result was present for both perceptions of credibility and investigatory resource allocation, thus the results are strong enough to reject the rival explanation.

Hypothesis six tests whether investigators negatively assess whistleblower credibility if they do not receive additional communication from a whistleblower beyond the submission of the initial report. The results of this test reveal that the lack of additional communication does negatively influence investigator perceptions of whistleblower credibility, which supports the hypothesized relationship. Therefore, it is important to encourage whistleblowers to maintain two-way communication with investigators in order to reduce the likelihood of an investigator perceiving the reported allegations as less credible simply due to a lack of communication.

The seventh hypothesis was assessed with contrast number five, which tests the theory that whistleblowers who respond, but indicate that they are either unwilling or unable to provide additional information will not experience any reduction in the investigator's perception of credibility. The result of this test does provide evidence that investigators' perception of credibility is not negatively impacted when the whistleblower states he or she is unable to provide any additional information.

The eighth and final hypothesis is perhaps the most telling. This test utilized contrast six to compare the credibility of anonymous whistleblowers who fully engaged in two-way communication, to that of identified whistleblowers who simply submitted their initial report. The results reveal that anonymous whistleblowers can be perceived as equally credible in the eyes of investigators by engaging in two-way communication

when compared to identified whistleblowers. This finding further supports the argument that two-way communication is critical to the success of effective whistleblowing and investigations, and therefore must be included in discussions of the credibility of anonymous whistleblowers.

Discussion

The results of this study (summarized in Table 3.16) clearly indicate that two-way communication must be considered in future discussions of the credibility of anonymous whistleblowers. First, this study has demonstrated that anonymous reports can be perceived to have the same level of credibility as identified reports. Second, a number of rival explanations have been investigated and found to have no confounding relationship with the impact of two-way communication on anonymous whistleblowing. The results of this study lead to a number of implications for both practice and future research.

Table 3.16 – Summary of Results

Hypothesis	Hypothesized Relationship	Sig.	Result
H1	Anonymous reports perceived as less credible	.001***	Supported
H2	More confidence in assessment for identified reports	.015**	Supported
H3	Fewer resources allocated to investigate anonymous reports	.892	Not Supported
H4a	Equal information results in equal credibility assessments	.809	Supported
H4b	Equal information results in equal allocations of resources	.212	Supported
H5a	Less information results in lower credibility	.062*	Supported
H5b	Less information results in lower allocation of resources	.031**	Supported
H6	Additional communication increases perceived credibility	.099*	Supported
H7	Reluctance to share information does not reduce credibility	.636	Supported
H8	Two-way communication reduces credibility gap	.112	Supported

NOTE: *** $p < 0.01$; ** $p < 0.05$; * $p < 0.10$

Practical Implications

Although research on two-way communication in whistleblowing currently lags behind its use in practice, the practical implications of this study are many. First, two-way communication provides excellent potential for improving the prospects of conducting effective investigations as anonymous reports may now be given proper consideration. Second, this study has further strengthened the argument against the use of open-door policies and telephone hotlines to report wrongdoing within organizations, as anonymous, computer-mediated, two-way communication provides greater anonymity protection without negatively impacting credibility. Third, this study has provided additional support for the efficacy of the ethics management system design proposed in Chapter 2. Lastly, further education should be provided to potential whistleblowers in order to encourage them to remain engaged in an active dialogue with investigators so that their report receives the maximum amount of consideration possible.

Research Implications

This study also leads to a number of implications for both past and future research. First, this study is the first to even suggest the use of two-way communication in the whistleblowing process. Therefore, the widely-held belief that anonymous whistleblowers aren't considered credible was simply limited due to the bounds of prior theories. By demonstrating the efficacy of two-way communication, this study has shown that previous theories failed to fully address the practical needs of both whistleblowers and investigators, which may have resulted in neglect for other critical whistleblowing research.

Second, whistleblowing has been widely studied in management, accounting and ethics, but little research has been conducted with respect to the technological aspects of this phenomenon. Therefore, this study provides an excellent spring board to propel its extension into areas of information systems research, such as computer-mediated communication, information security, and design science.

Third, since this study was able to reject a number of rival explanations which complicate the experimental design, simplified replications of this study can be extended to examine a wide variety of aspects which may impact investigators' perceived credibility and resource allocation, such as: (1) the seriousness of the alleged wrongdoing, (2) the various components of a whistleblowing report, and (3) whether the report is made internally or externally.

Fourth, rather than rely upon simulated communication, experiments with active participants serving the role of both whistleblower and investigator can be conducted to examine actual dialogue in order to gain a richer picture of such communication.

Lastly, the investigatory resource allocation trade-off decision can be extended to a within-subjects experiment which requires investigators to examine and simultaneously consider multiple reports of alleged wrongdoing. This would better represent a real-world situation for the investigator as he or she would be forced to allocate limited resources to investigate potential wrongdoing, which strengthens the generalizability of this research stream.

Conclusion

In conclusion, this chapter has reviewed existing theories in whistleblowing, as well as both inter-personal and computer-mediated communication, to argue for the

inclusion of two-way communication in whistleblowing research and practice. In doing so, this study addressed the limitations of prior theory regarding investigator perceptions of anonymous whistleblowers, while also empirically examining theorized relationships and rival explanations.

CHAPTER FOUR

PERCEPTIONS OF ANONYMITY PROTECTIONS

PROVIDED BY ETHICS MANAGEMENT

REPORTING CHANNELS

Introduction

This chapter assesses the design of an anonymous, two-way ethics management reporting system, proposed in Chapter 2, from the perspective of those who are likely to observe wrongdoing; that is, the organizational insider. In order to make a comprehensive assessment of the design, the proposed system is also compared to other reporting channels available to report wrongdoing, such as the use of open door policies and telephone hotlines. An online experiment with mixed designs was conducted to test user perceptions of each channel, as well as the specific whistleblower-oriented design features proposed in this dissertation. Theoretical justification is provided for each of the hypotheses under examination, results are discussed and implications for both practice and future research are outlined.

Theoretical Background

The theoretical justification for this study is grounded in prior research on anonymity and its role in disclosing wrongdoing. Each of the three reporting channels

under investigation is discussed in detail, which further informs the justification of the technical aspects of the proposed ethics management reporting system outlined in Chapter 2.

Anonymity vs. Confidentiality

As discussed in previous chapters, anonymity is only achieved when an individual's identity is not known (Elliston, 1981, 1982). This differs from related terms such as confidentiality. In the context of this dissertation, for example, confidentiality would involve keeping an identity, which is known to select number of individuals, secret from others unauthorized to know. Although employees who wish to disclose wrongdoing might have expectations of anonymity, the degree of anonymity a whistleblower can achieve is largely dependent upon the capabilities of the chosen reporting channel. The limitations of each channel will be discussed in the following section.

Limitations of Existing Reporting Channels

Open door policy. The intent of an open door policy is to encourage employees to speak to members of management rather than to withhold information by remaining silent. However, the extant research in this area shows how such policies might not produce the desired results if organizational culture does not match what is said in the employee handbook. As one might expect, employees are naturally hesitant to share negative news or opinions with management (Detert & Burris, 2007; Detert & Trevino, 2010; Miceli & Near, 1994; Morrison & Milliken, 2000), especially if it might reflect poorly on their standing within the organization (C. Park & Keil, 2009; Rosen & Tesser, 1970; H. J. Smith & Keil, 2003; Wang et al., 2015).

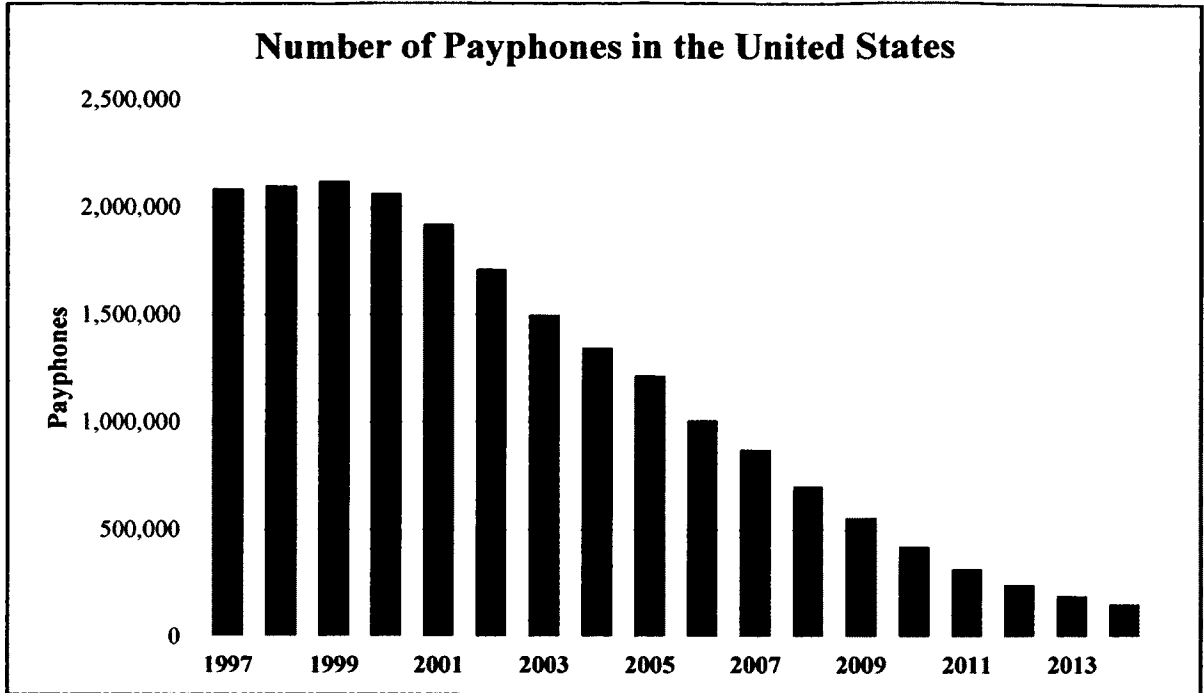
The Ethics Resource Center (2010) reports that an overwhelming majority (75%) of reports are made directly to either the employee's immediate supervisor (46%) or to higher management (29%). In light of these findings, it should come as no surprise that the reported rates of retaliation are high when considering the open door policy, at best, can only provide confidentiality. Therefore, anyone disclosing wrongdoing directly to a supervisor or member of management via an open door policy simply cannot expect any level of anonymity.

Phone hotline. Weaver, Trevino, & Cochran (1999) surveyed a population of Fortune 500 industrials and Fortune 500 service corporations, as they were listed in 1994. Of the 254 firms who responded, 51 percent reported the adoption of a telephone-based hotline or helpline in order to solicit questions and concerns from employees. While the use of phone hotlines through much of the 1990s might have been the only viable channel for providing some degree of anonymous, two-way communication, telephone-based systems have always been inherently vulnerable due to the fact that the caller's voice is likely recognizable, especially to those within the employee's organization. If the call is recorded, there are even more opportunities for others to attempt to identify the individual. Even attempts to distort the sound of someone's voice by using a voice synthesizer would not be sufficient to ensure adequate levels of anonymity for the technical reasons discussed next.

Today, the use of a phone hotline is even less likely to preserve anonymity due to the rise (and even decline) of other technologies. For example, every telephone call is routed through a highly regulated telecommunications network. At a minimum, the meta-data for each call, which includes the time, duration and phone numbers for all parties

involved, is documented and retained for a period of time by the telephone utility responsible for the network. While this information is primarily used to generate business records for customer billing purposes, the United States government has also demonstrated that such information is well within its reach (Landau, 2013, 2014; van Dijck, 2014). Therefore, all callers are at risk of being identified simply by the nature of telephone-based systems and data retention.

While the use of a public pay phone might have provided adequate degrees of anonymity for the caller at one point, the number of pay phones available in the United States has declined substantially in the past fifteen years (U.S. Federal Communications Commission, 2014); from a peak of 2.1 million in 1999 to just 152,716 in 2014 (See Figure 4.1). In addition, a determined party can now reference other sources, such as local surveillance cameras, in an effort to identify who made a particular call from a public location at a particular time. Therefore, the only option for obtaining a phone number which cannot be traced through business records would be to purchase a prepaid mobile phone. However, there are still many ways to determine who purchased the phone, especially if it is paid for using any type of electronic payment method.



**Figure 4.1 – Number of Payphones in the United States
(U.S. Federal Communications Commission, 2014)**

Another consideration that threatens, if not completely eliminates, any chance of achieving anonymity when reporting via a telephone-based hotline is the sheer volume of information generated, collected, transmitted and stored by mobile devices. For example, even if an individual were to use a public pay phone multiple states away, his or her location might be revealed simply due to traveling to the pay phone with a device that can determine a user's location (e.g., cell phone, vehicle navigation system). While many might point to the GPS function in mobile phones as the most obvious threat, a cellular mobile device's location can also be determined via triangulation of broadcast towers. Further, as more and more vehicles are equipped with GPS navigation, simply driving a car can generate a location log of travels.

While a single data point might not be enough to identify someone, the correlation of multiple data points can reveal a rather complete picture of an individual's activity (Biermann, 2011). To see how this can be achieved, simply review a six month period of Malte Spitz's life via German newspaper *Die Zeit Online*'s "Tell-all telephone" (2011) interactive map, which represents the 35,831 data points transmitted by Spitz's mobile phone over that period. Although attempts have been made to anonymize the traffic of Voice over IP (VoIP) telephone calls, such as with TORFone (<http://torfone.org>), the latency of such communications results in reduced audio quality, and an anonymous caller's voice might still be recognized. Therefore, without the ability to hide the information necessary to protect a caller's identity, the user is never able to reliably achieve anonymity via a telephone hotline.

Although not recommended, someone who is concerned about achieving the highest level of anonymity possible when reporting wrongdoing via a phone hotline, he or she must ensure that they: 1) purchase a disposable phone with cash that is only used for the purposes of reporting; 2) utilize a voice synthesizer or some other method to distort his or her voice; 3) remove the battery at all times when it is not in use; and 4) only make calls from public locations that are not in view of surveillance cameras. Performing all of these steps is time-consuming, costly, and involves some technical skill, yet still fails to reach the level of reliable anonymity protection necessary to protect against retaliation.

Online reporting system. With the advent of the Internet, most, if not all, human activity has found a comparable avenue online. This is also true for the reporting of wrongdoing. Although some systems existed prior to the passage of the *Sarbanes-Oxley*

Act (2002), most online reporting systems were developed in order to meet the needs of the market as all publicly-traded companies in the United States were now legally required by Sarbanes-Oxley to adopt an anonymous reporting channel. While many firms elected to maintain existing or even adopt new phone hotlines to satisfy this requirement, various online reporting systems were added to the portfolio. While online reporting systems do not require the user to speak, and therefore removes the possibility of recognizing a user by his or her voice, online systems are still vulnerable to similar location issues that phone hotlines experience (e.g., IP addresses). In addition, transitioning from telephone calls to Internet transmissions introduces a host of new threats to the protection of user anonymity. These threats to user anonymity and the proposed solutions for online reporting systems are discussed in the following section.

Proposed System Features

In Chapter 2, a number of system features were proposed for inclusion in the design of an anonymous ethics management reporting system. This study focuses on the features most likely to influence the organizational insider's (i.e., potential whistleblower) adoption of the system and excludes features which are aimed at assisting investigators. Therefore, the following system features are under investigation in this study: data encryption, Tor web browser, meta-data scrubbing, development method, and authentication.

Data encryption. A thorough discussion on the methods and uses of data encryption is provided in Chapter 2. Therefore, this section will discuss its role in the proposed system in a simplified, more practical sense. The use of data encryption in any system is to ensure unintended recipients are unable to decipher the contents of a

message, which provides secrecy rather than anonymity. In the case of the proposed system, end-to-end data encryption is employed from the user to the system server so that the identity and location of the user is not revealed. This feature is achieved by a combination of Transport Layer Security (TLS) and the Tor Anonymity Network, which is discussed in the following section.

Since the exit node removes the last layer of Tor encryption at the end of the Tor circuit, the exit node is capable of reading content that was not unencrypted prior to being transmitted through the Tor circuit. To protect against this, the data must be encrypted once more to remain secure for the entire circuit. Transport Layer Security is currently the asymmetric encryption standard for Internet traffic. While technically different from its predecessor, Secure Socket Layer (SSL) encryption, both approaches rely on public-key encryption. Therefore, each server offering encryption must publish a public key so that it is available to interested users. This provision allows anyone wishing to communicate with the server to encrypt the contents of the transmission with the public key, rendering the contents unreadable unless it is decrypted by the private key of the destination server. Furthermore, the use of Tor hidden services ensures that end-to-end encryption is achieved as it requires that separate Tor relays be established to a randomly selected rendezvous point prior to communicating. Therefore, the inclusion of this proposed system feature assists a user by protecting his or her anonymity through the secrecy afforded by data encryption.

Tor Browser Bundle. As previously discussed in Chapter 2, the use of a browser capable of an increased level of privacy and anonymity, such as the Tor Browser Bundle, is perhaps the most critical element of anonymous reporting via an online system. The

Tor Browser Bundle relies upon the Tor Anonymity Network in order to shield the user's digital identity. This identity blocking is accomplished by increasing the number of network "hops" between the sender and receiver. The Internet Protocol (IP) address associated with the user's device is obfuscated by enlisting the assistance of three randomly selected volunteer nodes on the Tor network, which provides the minimum number of hops between the sender and receiver in order for no single node to have knowledge of the entire path.

However, while necessary, increasing the number of hops alone is not sufficient. Without hiding the location of the nodes which form the Tor circuit, each of the volunteer nodes would be able to determine the full path from sender to receiver. Therefore, each transmission is encased in three layers of encryption, with each layer intended for one of the successive nodes in the circuit. The transmission can then only be decrypted by the intended node along the path. Each node then removes their layer of encryption, revealing the destination IP address of the next volunteer node, to which it forwards the transmission. This allows for the transmission to pass through the relay without a single node knowing the entire path due to the fact that the first node only knows the IP address of the sender and second node, the second node only knows the first and third, while the exit node only knows the second and intended recipient. Although Tor is vulnerable to certain attacks discussed in Chapter 2, such as timing analysis, intersection attacks and exit node sniffing, it provides the user with much greater anonymity protection than would be available with a standard browser.

Meta-data scrubbing. Meta-data is simply data which describe data. As discussed earlier, meta-data for a database of phone calls would likely consist of phone numbers,

time the call was placed, duration of the call and even information about the locations of the parties. Just as academia relies on blind peer-review to ensure fair and objective evaluation of research, anonymous whistleblowers need to be assured that the chosen channel will protect them from the threat of retaliation. Unfortunately, users who have clear and justifiable reasons for remaining anonymous might fail to remove meta-data from supporting documentation, which might inadvertently reveal their identities. For example, Young (2006) explains how the identity of a peer reviewer was unintentionally revealed to an author due to the meta-data stored in the Microsoft Word document which contained the reviewer's feedback.

While it would be wise for users to scrub any files of all meta-data prior to submission, it would be a disservice to the user not to include additional measures to automatically remove information which has the potential to compromise his or her identity. Therefore, whistleblowers that provide supporting documentation to support their allegations must have protections in place to ensure that such meta-data does not jeopardize their anonymity. There are limited tools currently available to incorporate directly into an online reporting system and it would be best for a custom solution to be developed for this purpose. However, one promising open-source application to consider is the Metadata Anonymisation Toolkit (MAT). A description of the program (<https://mat.boum.org/>) and the code repository (<https://gitweb.torproject.org/user/jvoisin/mat.git>) can be reviewed online.

Development method. The method of system development is perhaps the aspect of the proposed system design least likely to influence a user's perception of system anonymity. However, that does not mean it should not be or is any less critical in the case

of a reporting system. Open source development involves making the source code publically available for anyone to review, improve and use, free of cost (Cheng, Liu, & Tang, 2011; Lerner & Tirole, 2003; Rigby, Cleary, Painchaud, Storey, & German, 2012; von Krogh, Haefliger, Spaeth, & Wallin, 2012). In many cases, the code for open source projects can be found readily available in online repositories such as GitHub.com. This system allows for interested parties, even non-programmers, to monitor the project and suggest enhancements.

The primary advantage of open-source projects, as opposed to proprietary systems, is that the use of open source development provides greater transparency. In fact, system vulnerabilities are often identified and resolved more quickly in open source development due to the large community of volunteer contributors. Proprietary systems, on the other hand, do not afford users the opportunity to look behind the curtain and known system vulnerabilities might not be made public, putting users at risk. Unfortunately, the naïve user might not even be aware of the development method and find his or herself utilizing a proprietary system that does not adequately protect user anonymity. However, that is not to say all open source projects are always safer than all proprietary projects. Instead, proprietary system use simply raises the level of uncertainty in terms of system functionality, which is not acceptable for a system tasked with as complex a challenge as protecting user anonymity.

Authentication. The proposed design also advocates the use of system-generated passphrases for the purposes of user authentication. Authentication is necessary to facilitate anonymous, two-way communication since the user must be able to reference his or her prior report(s). The use of a system-generated passphrase, as opposed to one

provided by the user, ensures that the user does not naively enter anything that can be connected to their identity. For example, if the reporting system is implemented within an organization for the purposes of internal reporting, the organization would be able to access the user passwords for other systems and match them to the ones used to report wrongdoing via the reporting system. Due to the challenge of remembering multiple passwords, users are unlikely to create unique authentication credentials for each system they use, which only increases the threat (Adams & Sasse, 1999; Hayashi & Hong, 2011; Ives, Walsh, & Schneider, 2004; Zhang, Luo, Akkaladevi, & Ziegelmeier, 2009; Zviran & Haga, 1999). By preventing the user from submitting their own and forcing them to select a randomly generated passphrase to associate with their report, the user has been protected against a potential threat to his or her anonymity.

Research Questions

The prior discussion of the existing literature raises the following research questions: (1) *How are the existing reporting channels perceived by employees?*; (2) *What is the adoption intention for each of the existing reporting channels?*; (3) *Which of the proposed system features influence employees' perception of anonymity protections?*; (4) *Would the adoption of the proposed online reporting system increase employees' likelihood of blowing the whistle?*

Hypotheses Development

Formal hypotheses have been developed to test each of these research questions, and they will be outlined and discussed in detail in the following section.

Reporting Channels

Before assessing the specifics of the proposed system design, it is first necessary to assess user perceptions of each of the three reporting channels in general. As discussed in earlier sections, the best protection an open door policy can provide is confidentiality, which is not sufficient for protecting against retaliation. Further, phone hotlines are vulnerable to a number of technical issues which might reveal the identity of a caller. Therefore, it is expected that users will perceive online reporting systems to provide greater anonymity protections than open door policies and phone hotlines. Three specific perceptions of anonymity protections are tested for each reporting channel in hypotheses H1, H2 and H3. The subdimensions of anonymity under examination consist of knowledge of others, system functionality and lack of identification.

- H1: The online system will be perceived as more likely to maintain anonymity with respect to the knowledge of others when compared to user perceptions of the:
 - a) Open Door Policy
 - b) Phone Hotline

- H2: The online system will be perceived as more likely to function as expected with respect to preserving anonymity of the user when compared to the user perceptions of the:
 - a) Open Door Policy
 - b) Phone Hotline

- H3: The online system will be perceived as more likely to maintain anonymity with respect to lack of identification of the user when compared to the user perceptions of the:
 - a) Open Door Policy
 - b) Phone Hotline

Further, it can be expected that the phone hotline will be perceived as providing greater anonymity protections for each of the three subdimensions than can be offered by the open door policy. Although not a primary focus of this study, this expected relationship is also tested in hypothesis 4 in an effort to thoroughly examine the perceptions of each reporting channel.

- H4: The phone hotline will be perceived as more likely to maintain anonymity than the open door policy, with respect to:
- a) Knowledge of others
 - b) Functioning as expected
 - c) Lack of identification

System Features

Although the technical capabilities provided by the proposed features are known to enhance anonymity protection for the user, system designers must be aware of whether users can understand the technical capabilities of the system. Otherwise, naïve users are unlikely to adopt the reporting channel best suited to protect them. Therefore, hypotheses H5 through H9 will test whether the presence of enhanced features increases user perceptions of anonymity protections provided by the proposed online reporting system.

- H5: The proposed use of the Tor web browser increases user perceptions of anonymity protections provided by the system.
- H6: The proposed use of end-to-end data encryption increases user perceptions of anonymity protections provided by the system.
- H7: The proposed scrubbing of meta-data increases user perceptions of anonymity protections provided by the system.
- H8: The proposed use of open source development increases user perceptions of anonymity protections provided by the system.

- H9: The proposed use of system-generated passphrases increases user perceptions of anonymity protections provided by the system.

Methodology

The target sample for this study consisted of full-time employees who were currently working for a single employer located within the United States, as they serve as the pool of potential whistleblowers who might report misconduct within organizations. Study subjects were invited to participate in the experiment after successfully qualifying through the use of a demographic survey.

Participants were recruited and compensated via Amazon's Mechanical Turk (MTurk) crowdsourcing platform (Buhrmester, Kwang, & Gosling, 2011). The reliability of data obtained via MTurk workers has been shown to be at least as reliable as other online methods (Ayyagari, Grover, & Purvis, 2011) and potentially more reliable than traditional subject pools (Behrend, Sharek, Meade, & Wiebe, 2011; Buhrmester et al., 2011; Casler, Bickel, & Hackett, 2013). MTurk has also been shown to provide samples that are as representative of the U.S. population when compared to samples obtained from students (Paolacci, Chandler, & Ipeirotis, 2010). In terms of diversity, MTurk samples are more likely to exhibit representative distributions in term of age, ethnicity, and work experience (Behrend et al., 2011). Non-qualifiers were compensated \$0.10 in exchange for participating in the qualification portion of the study. Those who qualified and completed the study were compensated at an average hourly rate of \$7.80 (USD) based upon the average completion time of 25 minutes.

Two experimental designs, which were conducted simultaneously, were employed to investigate the research questions for this study. First, perceptions of three reporting channels were tested via a 1 x 3 within-subjects design. After responding to measures of

employee silence developed by Knoll & van Dick (2013), participants were asked to evaluate descriptions of an open-door policy (Table 4.1), phone hotline (Table 4.2), and a variation of an online reporting system. Accordingly, the system features for the proposed ethics management reporting system were tested using a randomized 2⁵ factorial design (Table 4.3). User perceptions of each reporting channel (hypotheses 1-4) were compared using paired T-tests, and Multivariate Analysis of Covariance (MANCOVA) was conducted to assess the impact of each of the proposed features on the perceptions of anonymity protection provided by online reporting systems. This mixed-method design allowed for comparisons to be made among all three channels, as well as test the specific system characteristics in order to determine which features influence user perceptions of anonymity with respect to online reporting systems.

Following the evaluation of reporting channels, participants were then asked to review and evaluate a randomly assigned scenario adopted from McMahon & Harvey (2006). Each of the three scenarios consisted of a moral intensity manipulation (high vs. low) in order to test the intent of participants to report the wrongdoing (Table 4.4). Respondents evaluated the perceived moral intensity (McMahon & Harvey, 2006) of the behavior exhibited in the scenario, as well as provided their perception of the risk of reporting the wrongdoing (Lowry et al., 2013). After participants reviewed the scenario, whistleblowing intentions were assessed using the scale developed by H. Park & Blenkinsopp (2008).

Table 4.1 – Description of the Open Door Policy

Open Door Policy
<p>Assume that your organization has stated that they are committed to creating a work environment where everyone's voice is heard, where issues are promptly raised and resolved, and where communication flows across all levels of the company. Openness is essential to quickly resolve customer concerns, to recognize business issues as they arise, and to address the changing needs of a diverse workforce.</p> <p>Therefore, also assume your organization has encouraged managers to be available and approachable via an “open door policy” in order for employees to feel safe in reporting issues directly to management. This method of reporting provides an opportunity for an active dialogue to take place between managers and their subordinates.</p> <p>In accordance with company policy, if an employee so chooses, the identity of any employee who shares information with a superior via the open door policy must remain confidential.</p>

Table 4.2 – Description of the Phone Hotline

Phone Hotline
<p>Assume that a telephone hotline may be used to report issues directly to your organization’s internal compliance department. The hotline can be accessed 24 hours a day and seven days a week by dialing a dedicated phone number, but a compliance officer may not be available to answer the call at all times. If the call cannot be answered, the employee may leave a voice recording of the issue and a member of the compliance department will review the issue within 24 hours.</p> <p>An employee using the telephone hotline may elect to withhold his or her name when submitting their report. If an employee's identity is provided, the compliance department is required to keep it confidential.</p> <p>An anonymous report can be followed up with during subsequent calls by referencing the case number automatically generated by the phone hotline system, which is provided to the employee when making his or her initial report.</p>

Table 4.3 – Manipulations Employed in the Online Reporting System Description

FEATURE	LEVEL A (Proposed Feature)	LEVEL B (Control)
STANDARD TEXT	<p>Assume that an online reporting system is available for employees in your organization to raise concerns 24 hours a day and seven days a week. While a compliance officer may not be available to respond immediately at all times, a member of the compliance department will respond via the system within 24 hours.</p>	
BROWSER	<p>The system can only be accessed when using a free, open-source web browser designed to anonymize a user's online activity. This is achieved by routing the encrypted communication via a random path of network nodes between the sending and receiving devices, which prevents the reporting system from being provided with the user's IP address.</p>	<p>The system can be accessed when using any standard web browser (e.g., Internet Explorer, Google Chrome, Mozilla Firefox). When accessing any website from a standard browser, it is possible for the IP address of the user's device to be logged by the server. However, the organization promises that no such data will actually be collected by the system.</p>
ENCRYPTION	<p>Data handled by the system is encrypted from end-to-end. The purpose of end-to-end encryption is to prevent any intermediaries and/or unintended recipients from being able to discover or tamper with the content of the communications between the employee and investigator.</p>	<p>Data handled by the system is not encrypted from end-to-end. The purpose of end-to-end encryption is to prevent any intermediaries and/or unintended recipients from being able to discover or tamper with the content of the communications between the employee and investigator.</p>
META-DATA	<p>Employees may elect to upload file attachments when submitting their report. Any such supporting documentation associated with a report will be automatically scrubbed of any document property meta-data, such as author and date created, prior to being provided to investigators.</p>	<p>Employees may elect to upload file attachments when submitting their report. Any such supporting documentation associated with a report will be provided to investigators in its original and unaltered form.</p>
DEVELOPMENT	<p>The system is an open-source development project. The code is publicly available online. A team of volunteers around the world is responsible for finding any vulnerabilities and making enhancements to the system.</p>	<p>The system is a proprietary development project. The code is not publicly available online. A team of paid employees is responsible for finding any vulnerabilities and making enhancements to the system.</p>
PASSPHRASE	<p>The system is capable of two-way communication between the employee and investigator. Anonymous employees can access messages from the investigator, as well as check the status of a previously submitted report, by entering the system-generated passphrase that was provided to the employee prior to submitting the initial report.</p>	<p>The system is capable of two-way communication between the employee and investigator. Anonymous employees can access messages from the investigator, as well as check the status of a previously submitted report, by entering the user-provided passphrase that was entered by the employee prior to submitting the initial report.</p>

Table 4.4 – Scenarios

Scenario	Low Intensity	High Intensity
Office Supplies (adapted from McMahon & Harvey, 2006)	An employee in charge of ordering office supplies for your firm discovered a box of staples that was not ordered in the week's shipment of supplies and did not appear on the invoice. The employee decided not to tell the office supply company about the mistake and took the staples home.	An employee in charge of ordering office supplies for your firm discovered a laptop computer that was not ordered in the week's shipment of supplies and did not appear on the invoice. The employee decided not to tell the office supply company about the mistake and took the computer home.
New Market (adapted from McMahon & Harvey, 2006; originally adapted from Fritzsche & Becker, 1984)	Your firm is considering opening a facility in an underdeveloped country that appears to be poised for rapid growth. Initial contacts with officials in the country left no doubt that approval of your firm's entry into the market would require a contribution to the ruling political party. Other firms have also attempted to enter the market, some of which have made a contribution, and some of which have cancelled their plans because of their refusal to pay a contribution. You learn that the CEO of your firm has approved payment of the contribution.	Your firm is considering opening a facility in an underdeveloped country that appears to be poised for rapid growth. Initial contacts with officials in the country left no doubt that approval of your firm's entry into the market would require a contribution to the ruling political party. Every other firm that has attempted to enter the market has decided against it, because making the contribution was a business practice in which they did not wish to engage. You learn that the CEO of your firm has approved payment of the contribution.
Computer Software (adapted from McMahon & Harvey, 2006)	One of your coworkers recently decided to buy a new personal computer for home use. A state-of-the-art computer was purchased at a very affordable price, but the trade-off for getting a low price was that it came with a very limited amount of pre-loaded software. Even though it is against company policy, your colleagues have mixed opinions about using unlicensed software. You learn that in order to avoid purchasing a personal license for certain software, your coworker has decided to install software, licensed exclusively to your workplace, onto the new home computer for personal use.	One of your coworkers recently decided to buy a new personal computer for home use. A state-of-the-art computer was purchased at a very affordable price, but the trade-off for getting a low price was that it came with a very limited amount of pre-loaded software. Your colleagues strongly support the company's policy of purchasing of a separate license for every computer on which a piece of software will be installed. However, you learn that in order to avoid purchasing a personal license for certain software, your coworker has decided to install software, licensed exclusively to your workplace, onto the new home computer for personal use.

Manipulation Checks

To ensure that the manipulated descriptions of the online reporting system were recognized by the participants, a single item was used for each of the five features under examination. Based upon the results provided in Table 4.5, the manipulations proved effective for each of the five system features.

Table 4.5 – System Feature Manipulation Checks

ANOVA						
Feature	Source	Sum of Squares	Df	Mean Square	F	Sig.
Browser	Between Groups	282.583	1	282.583	168.080	.000***
	Within Groups	677.540	403	1.681		
	Total	960.123	404			
Encryption	Between Groups	531.306	1	531.306	316.208	.000***
	Within Groups	677.138	403	1.680		
	Total	1208.444	404			
Meta-Data	Between Groups	206.431	1	206.431	151.769	.000***
	Within Groups	548.147	403	1.360		
	Total	754.578	404			
Development	Between Groups	279.250	1	279.250	199.745	.000***
	Within Groups	563.407	403	1.398		
	Total	842.657	404			
Passphrase	Between Groups	217.127	1	217.127	119.847	.000***
	Within Groups	730.117	403	1.812		
	Total	947.244	404			

NOTE: *** p < 0.01; ** p < 0.05; * p < 0.10

Measures

A multiple-group confirmatory factor analysis (CFA) was conducted using IBM® SPSS® Amos on three subdimensions of the Confidence in Whistleblowing Reporting

System measure employed by (Lowry et al., 2013) in order to assess participants' perception of the anonymity provided by each of the three reporting channels. The three subdimensions consist of Knowledge of Others, System Functionality and Lack of Identification.

As expected, the results of the tests for metric invariance indicated that the models for each reporting channel were significantly different. Therefore, the factor structure was analyzed separately for each reporting channel. The model fit for the CFA conducted for each reporting channel is provided in Table 4.6. However, the measure performed poorly in terms of discriminant validity as the average variance extracted (AVE) was lower for each construct's squared correlation estimate. In order to further test the underlying theory, the fit for multiple models was compared. The one factor model, as well as models with some or all construct correlations fixed to 1, all exhibited worse fit than the theoretical 3-factor model proposed by Lowry et al. (2013). According to Hair, Black, Babin, & Anderson (2009), this result provides evidence that the original model is preferred, despite the limited discriminant validity. The factor structure of the measure for each of the three reporting channels is reproduced in Table 4.7.

Table 4.6 – Model Fit for the Confidence in Reporting Channel Anonymity CFA

Statistic	Open Door Policy	Phone Hotline	Online System
Chi-Square (df)	296.43 (84) ***	291.77 (85) ***	233.98 (83) ***
RMSEA	.079	.078	.067
GFI	.911	.910	.930
CFI	.951	.948	.966

Table 4.7 – Online Reporting System Anonymity

Item	Online System			Phone Hotline			Open Door Policy		
	KNW	FNC	LID	KNW	FNC	LID	KNW	FNC	LID
I believe others would be able to identify my report if I used the online reporting system.	.648			.728			.637		
I believe that those who investigate reports do not know others well enough to identify the source of the reports provided via the online reporting system.	.744			.767			.728		
I believe I would not have distinguishing characteristics that would allow other participants to identify my reports when reporting via the online reporting system.	.814			.794			.770		
I believe it would be possible to identify the origin of the reports based upon the author's personal characteristics when using online reporting system.	.604			.667			.584		
I would not recognize the author of most reports if they were provided via the online reporting system.	.723			.747			.800		
I believe the group of potential employees is large enough that it would be impossible for anyone to identify my reports if submitted via the online reporting system.	.845			.804			.800		
I believe the online reporting system would not malfunction and identify me as the source of my comments.	.691			.612			.753		
I believe it would not be possible to identify me as the source of my comments using the online reporting system.	.786			.754			.747		
I believe that the online reporting system would not store any technical information with my comments that would allow for the source to be identified.	.764			.695			.652		
Unless intentionally provided by the source, I believe that no names would be attached to the reports submitted via online reporting system.	.782			.648			.767		
I believe that my comments would not be identified in the online reporting system.	.838			.842			.814		
When using the online reporting system, my personal identity would not be provided in the report unless I chose to provide it.			.762			.640			.756
During the process of reporting via the online reporting system, no one could know who is reporting the issue unless the source intentionally reveals their identity.			.881			.861			.847
My reporting via the online reporting system would be entirely secret if I wanted it to be.			.879			.870			.879
No personally identifying information would be found in my reports unless I provided it when using the online reporting system.			.791			.748			.819
Variance Extracted 54.0% 59.9% 68.9% 56.6% 51.1% 61.7% 52.5% 56.0% 68.3% Composite Reliability .874 .881 .898 .886 .838 .864 .867 .864 .896									

Results

Sample Demographics

The total usable sample of 405 respondents consisted of 61% males (Table 4.8), with an average age of 34 years, ranging from 19 to 70 years old (Table 4.9). All participants were employed with a single employer and over 43% have attained a bachelor's degree (Table 4.10). Organizational tenure, organization type and industry are provided in Table 4.11, Table 4.12, and Table 4.13, respectively.

Table 4.8 – Sample Gender

Gender	Frequency	Percent
Males	247	61.0
Females	158	39.0
Total	405	100.0

Table 4.9 – Sample Age

Age (in years)	Frequency	Percent	Cumulative Percent
< 20	1	0.2	.2
20 – 29	153	37.8	38.0
30 – 39	160	39.5	77.5
40 – 49	57	14.1	91.6
50 – 59	29	7.2	98.8
60 – 69	4	1.0	99.8
> 70	1	0.2	100.0
Total	405	100.0	

Table 4.10 – Sample Education Level

Type	Frequency	Percent	Cumulative Percent
High School / GED	39	9.6	9.6
Some College	95	23.5	33.1
Associate's Degree	41	10.1	43.2
Bachelor's Degree	175	43.2	86.4
Master's Degree	49	12.1	98.5
Doctoral Degree	3	0.7	99.3
Professional Degree (JD, MD)	3	0.7	100.0
Total	405	100.0	

Table 4.11 – Organizational Tenure

Tenure (in years)	Frequency	Percent	Cumulative Percent
0 – 1	58	14.3	14.3
2 – 3	99	24.4	38.8
4 – 5	97	24.0	62.7
6 – 7	46	11.4	74.1
8 – 9	35	8.6	82.7
10 – 11	30	7.4	90.1
12 – 13	15	3.7	93.8
14 – 15	9	2.2	96.0
16 – 17	7	1.7	97.8
> 18	9	2.2	100.0
Total	405	100.0	

Table 4.12 – Type of Organization

Type	Frequency	Percent	Cumulative Percent
Private, For-Profit	292	72.1	72.1
Private, Not-For-Profit	23	5.7	77.8
Public, For-Profit	38	9.4	87.2
Public, Not-For-Profit	19	4.7	91.9
Local Government	11	2.7	94.6
State Government	13	3.2	97.8
Federal Government	8	2.0	99.8
Self-Employed	1	0.2	100.0
Total	405	100.0	

Table 4.13 – Industry

Industry	Frequency	Percent	Cumulative Percent
Agriculture	1	0.2	0.2
Accounting	6	1.5	1.7
Advertising	6	1.5	3.2
Automotive	5	1.2	4.4
Banking	10	2.5	6.9
Broadcasting	1	0.2	7.2
Biotechnology	2	0.5	7.7
Chemical	2	0.5	8.1
Consulting	6	1.5	9.6
Consumer Products	3	0.7	10.4
Defense	2	0.5	10.9
Education	42	10.4	21.2
Energy	2	0.5	21.7
Entertainment & Leisure	13	3.2	24.9
Financial Services	33	8.1	33.1
Food, Beverage & Tobacco	16	4.0	37.0
Grocery	2	0.5	37.5
Health Care	51	12.6	50.1
Legal	7	1.7	51.9
Manufacturing	24	5.9	57.8
Pharmaceuticals	4	1.0	58.8
Publishing	2	0.5	59.3
Real Estate	8	2.0	61.2
Retail & Wholesale	40	9.9	71.1
Service	23	5.7	76.8
Technology	46	11.4	88.1
Telecommunications	7	1.7	89.9
Television	2	0.5	90.4
Transportation	16	4.0	94.3
Other	23	5.7	100.0
Total	405	100.0	

Hypothesis Tests

Hypotheses 1 through 4 were assessed using paired T-tests of each reporting channel. The results are provided in Table 4.14. A Multivariate Analysis of Covariance (MANCOVA) was conducted to test hypotheses 5 through 9. The between-effects output is reproduced in Table 4.15. A summary of all results can be found in Table 4.16.

Table 4.14 – Paired Samples Test of Reporting Channel Perceptions

		Paired Samples Test					t	df	Sig. (2-tail)
Hyp.	Tested Pair	Paired Differences							
		Mean Diff.	Std. Dev.	Std. Error Mean	95% Con. Interval of the Diff.				
					Lower	Upper			
H1a	Online System Knowledge – Open Door Knowledge	0.965	1.577	0.078	0.811	1.119	12.322	404	.000***
H1b	Online System Knowledge – Phone Hotline Knowledge	0.764	1.698	0.084	0.599	0.930	9.062	404	.017**
H2a	Online System Function – Open Door Function	0.412	1.487	0.074	0.266	0.557	5.571	404	.000***
H2b	Online System Function – Phone Hotline Function	0.176	1.461	0.073	0.033	0.318	2.422	404	.033**
H3a	Online System Lack of ID – Open Door Lack of ID	0.554	1.517	0.075	0.406	0.702	7.349	404	.000***
H3b	Online System Lack of ID – Phone Hotline Lack of ID	0.589	1.598	0.079	0.433	0.745	7.412	404	.014**
H4a	Phone Hotline Knowledge – Open Door Knowledge	0.955	1.827	0.091	0.776	1.133	10.516	404	.000***
H4b	Phone Hotline Function – Open Door Function	0.259	1.574	0.078	0.105	0.412	3.307	404	.000***
H4c	Phone Hotline Lack of ID – Open Door Lack of ID	0.696	1.768	0.088	0.524	0.869	7.926	404	.000***

NOTE: * p < 0.01; ** p < 0.05;**

Table 4.15 – Tests of Between-Subjects Effects for Proposed System Features

Source	Dependent Variable	Type III Sum of Squares	Df	Mean Square	F	Sig.
CORRECTED MODEL	Knowledge of Others	97.848	34	2.878	1.857	.003
	System Functionality	100.942	34	2.969	1.801	.005
	Lack of Identification	93.340	34	2.745	1.550	.028
INTERCEPT	Knowledge of Others	357.851	1	357.851	230.890	.000
	System Functionality	414.135	1	414.135	251.268	.000
	Lack of Identification	382.261	1	382.261	215.794	.000
AGE	Knowledge of Others	.267	1	.267	.173	.678
	System Functionality	2.467	1	2.467	1.497	.222
	Lack of Identification	.475	1	.475	.268	.605
GENDER	Knowledge of Others	3.232	1	3.232	2.086	.150
	System Functionality	6.408	1	6.408	3.888	.049**
	Lack of Identification	.503	1	.503	.284	.594
EDUCATION	Knowledge of Others	4.962	1	4.962	3.202	.074*
	System Functionality	2.030	1	2.030	1.232	.268
	Lack of Identification	.501	1	.501	.283	.595
BROWSE	Knowledge of Others	8.830	1	8.830	5.697	.017**
	System Functionality	10.845	1	10.845	6.580	.011**
	Lack of Identification	16.389	1	16.389	9.252	.003**

Table 4.15 – Tests of Between-Subjects Effects for Proposed System Features (Continued)

Source	Dependent Variable	Type III Sum of Squares	Df	Mean Square	F	Sig.
ENCRYPT	Knowledge of Others	5.846	1	5.846	3.772	.053*
	System Functionality	3.790	1	3.790	2.300	.130
	Lack of Identification	7.548	1	7.548	4.261	.040**
META	Knowledge of Others	6.045	1	6.045	3.900	.049**
	System Functionality	9.897	1	9.897	6.005	.015**
	Lack of Identification	9.085	1	9.085	5.129	.024**
DEV	Knowledge of Others	1.539	1	1.539	.993	.320
	System Functionality	2.453	1	2.453	1.489	.223
	Lack of Identification	3.186	1	3.186	1.799	.181
PASS	Knowledge of Others	1.339	1	1.339	.864	.353
	System Functionality	.002	1	.002	.001	.973
	Lack of Identification	.317	1	.317	.179	.673
BROWSE * ENCRYPT	Knowledge of Others	3.482	1	3.482	2.247	.135
	System Functionality	1.676	1	1.676	1.017	.314
	Lack of Identification	1.927	1	1.927	1.088	.298
BROWSE * META	Knowledge of Others	11.683	1	11.683	7.538	.006**
	System Functionality	3.151	1	3.151	1.912	.168
	Lack of Identification	9.776	1	9.776	5.519	.019**

Table 4.15 – Tests of Between-Subjects Effects for Proposed System Features (Continued)

Source	Dependent Variable	Type III Sum of Squares	Df	Mean Square	F	Sig.
BROWSE * DEV	Knowledge of Others	.299	1	.299	.193	.661
	System Functionality	.107	1	.107	.065	.799
	Lack of Identification	.147	1	.147	.083	.773
BROWSE * PASS	Knowledge of Others	5.309	1	5.309	3.426	.065*
	System Functionality	6.448	1	6.448	3.912	.049**
	Lack of Identification	6.775	1	6.775	3.825	.051*
ENCRYPT * META	Knowledge of Others	.001	1	.001	.001	.979
	System Functionality	1.538	1	1.538	.933	.335
	Lack of Identification	.184	1	.184	.104	.748
ENCRYPT * DEV	Knowledge of Others	.002	1	.002	.001	.971
	System Functionality	1.556	1	1.556	.944	.332
	Lack of Identification	1.192	1	1.192	.673	.413
ENCRYPT * PASS	Knowledge of Others	2.868	1	2.868	1.850	.175
	System Functionality	1.851	1	1.851	1.123	.290
	Lack of Identification	2.218	1	2.218	1.252	.264
META * DEV	Knowledge of Others	.014	1	.014	.009	.923
	System Functionality	.000	1	.000	.000	.998
	Lack of Identification	.401	1	.401	.226	.634

Table 4.15 – Tests of Between-Subjects Effects for Proposed System Features (Continued)

Source	Dependent Variable	Type III Sum of Squares	Df	Mean Square	F	Sig.
META * PASS	Knowledge of Others	.782	1	.782	.504	.478
	System Functionality	3.420	1	3.420	2.075	.151
	Lack of Identification	1.040	1	1.040	.587	.444
DEV * PASS	Knowledge of Others	.006	1	.006	.004	.951
	System Functionality	.056	1	.056	.034	.854
	Lack of Identification	.432	1	.432	.244	.622
BROWSE * ENCRYPT * META	Knowledge of Others	12.517	1	12.517	8.076	.005**
	System Functionality	7.162	1	7.162	4.346	.038**
	Lack of Identification	14.005	1	14.005	7.906	.005**
BROWSE * ENCRYPT * DEV	Knowledge of Others	.231	1	.231	.149	.699
	System Functionality	6.175	1	6.175	3.747	.054*
	Lack of Identification	1.916	1	1.916	1.082	.299
BROWSE * ENCRYPT * PASS	Knowledge of Others	8.548	1	8.548	5.515	.019**
	System Functionality	4.842	1	4.842	2.938	.087*
	Lack of Identification	3.739	1	3.739	2.110	.147
BROWSE * META * DEV	Knowledge of Others	.868	1	.868	.560	.455
	System Functionality	.002	1	.002	.001	.971
	Lack of Identification	.305	1	.305	.172	.679

Table 4.15 – Tests of Between-Subjects Effects for Proposed System Features (Continued)

Source	Dependent Variable	Type III Sum of Squares	Df	Mean Square	F	Sig.
BROWSE * META * PASS	Knowledge of Others	.057	1	.057	.037	.848
	System Functionality	.417	1	.417	.253	.615
	Lack of Identification	.311	1	.311	.176	.675
BROWSE * DEV * PASS	Knowledge of Others	4.225	1	4.225	2.726	.100
	System Functionality	.309	1	.309	.188	.665
	Lack of Identification	.649	1	.649	.367	.545
ENCRYPT * META * DEV	Knowledge of Others	.035	1	.035	.023	.880
	System Functionality	.064	1	.064	.039	.844
	Lack of Identification	.040	1	.040	.022	.881
ENCRYPT * META * PASS	Knowledge of Others	1.345	1	1.345	.868	.352
	System Functionality	.024	1	.024	.015	.904
	Lack of Identification	.004	1	.004	.002	.963
ENCRYPT * DEV * PASS	Knowledge of Others	2.724	1	2.724	1.757	.186
	System Functionality	3.602	1	3.602	2.185	.140
	Lack of Identification	1.374	1	1.374	.776	.379
META * DEV * PASS	Knowledge of Others	2.632	1	2.632	1.698	.193
	System Functionality	.100	1	.100	.061	.805
	Lack of Identification	.280	1	.280	.158	.691

Table 4.15 – Tests of Between-Subjects Effects for Proposed System Features (Continued)

Source	Dependent Variable	Type III Sum of Squares	Df	Mean Square	F	Sig.
	Knowledge of Others	.033	1	.033	.021	.885
BROWSE * ENCRYPT * META * DEV	System Functionality	.024	1	.024	.015	.904
	Lack of Identification	.000	1	.000	.000	.992
	Knowledge of Others	3.310	1	3.310	2.135	.145
BROWSE * ENCRYPT * META * PASS	System Functionality	4.030	1	4.030	2.445	.119
	Lack of Identification	2.527	1	2.527	1.426	.233
	Knowledge of Others	.162	1	.162	.104	.747
BROWSE * ENCRYPT * DEV * PASS	System Functionality	.205	1	.205	.124	.725
	Lack of Identification	.261	1	.261	.147	.702
	Knowledge of Others	.432	1	.432	.279	.598
BROWSE * META * DEV * PASS	System Functionality	2.589	1	2.589	1.571	.211
	Lack of Identification	2.132	1	2.132	1.203	.273
	Knowledge of Others	.029	1	.029	.019	.892
ENCRYPT * META * DEV * PASS	System Functionality	.520	1	.520	.316	.575
	Lack of Identification	.303	1	.303	.171	.680
	Knowledge of Others	.208	1	.208	.134	.714
BROWSE * ENCRYPT * META * DEV * PASS	System Functionality	2.451	1	2.451	1.487	.223
	Lack of Identification	1.072	1	1.072	.605	.437

Table 4.15 – Tests of Between-Subjects Effects for Proposed System Features (Continued)

Source	Dependent Variable	Type III Sum of Squares	Df	Mean Square	F	Sig.
ERROR	Knowledge of Others	573.454	370	1.550		
	System Functionality	609.826	370	1.648		
	Lack of Identification	655.424	370	1.771		
TOTAL	Knowledge of Others	8883.056	405			
	System Functionality	9818.680	405			
	Lack of Identification	11231.875	405			
CORRECTED TOTAL	Knowledge of Others	671.302	404			
	System Functionality	710.768	404			
	Lack of Identification	748.763	404			

a. $R^2 = .146$ (Adjusted $R^2 = .067$) b. $R^2 = .142$ (Adjusted $R^2 = .063$) c. $R^2 = .125$ (Adjusted $R^2 = .044$) d. Computed using alpha = .05
NOTE: *** p < 0.01; ** p < 0.05; * p < 0.10

Table 4.16 – Summary of Results

Hypothesis	Hypothesized Relationship	Result
H1a	Perceived Knowledge of Others for Online System > Open Door Policy	.000***
H1b	Perceived Knowledge of Others for Online System > Phone Hotline	.017**
H2a	Perceived Channel Functionality for Online System > Open Door Policy	.000***
H2b	Perceived Channel Functionality for Online System > Phone Hotline	.033**
H3a	Perceived Lack of Identification for Online System > Open Door Policy	.000***
H3b	Perceived Lack of Identification for Online System > Phone Hotline	.014**
H4a	Perceived Knowledge of Others for Phone Hotline > Open Door Policy	.000***
H4b	Perceived Channel Functionality for Phone Hotline > Open Door Policy	.000***
H4c	Perceived Lack of Identification for Phone Hotline > Open Door Policy	.000***
H5a	Tor Browser increases Perceived Channel Anon.: Knowledge of Others	.017**
H5b	Tor Browser increases Perceived Channel Anon.: Channel Functionality	.011**
H5c	Tor Browser increases Perceived Channel Anon.: Lack of Identification	.003**
H6a	Data encryption increases Perc. Channel Anon.: Knowledge of Others	.053*
H6b	Data encryption increases Perc. Channel Anon.: Channel Functionality	N/S
H6c	Data encryption increases Perc. Channel Anon.: Lack of Identification	.040**
H7a	Meta-data scrubbing increases Perc. Channel Anon.: Knowledge of Others	.049**
H7b	Meta-data scrubbing increases Perc. Channel Anon.: Channel Functionality	.015**
H7c	Meta-data scrubbing increases Perc. Channel Anon.: Lack of Identification	.024**
H8a	Open source dev. increases Perc. Channel Anon: Knowledge of Others	N/S
H8b	Open source dev. increases Perc. Channel Anon: Channel Functionality	N/S
H8c	Open source dev. increases Perc. Channel Anon: Lack of Identification	N/S
H9a	System passphrase increases Perc. Channel Anon.: Knowledge of Others	N/S
H9b	System passphrase increases Perc. Channel Anon.: Channel Functionality	N/S
H9c	System passphrase increases Perc. Channel Anon.: Lack of Identification	N/S
H10	Employee Silence increases Perceived Risk of Reporting	.000***
H11	Perceived System Anonymity decreases Perceived Risk of Reporting	.098*
H12	Perceived Risk of Reporting decreases Internal Whistleblowing Intentions	.000***
H13	Perceived Risk of Reporting increases External Whistleblowing Intentions	.000***

NOTE: *** p < 0.01; ** p < 0.05; * p < 0.10

Discussion

Perceptions of Reporting Channels

This study has confirmed that users perceive online reporting systems as providing more anonymity protection than phone hotlines and open door policies. Despite this encouraging result, 75 percent of employees still elect to report to a member of management within the organization (Ethics Resource Center, 2010). Therefore, it is critical that employees understand that the best defense against retaliation is reporting via an online system which can provide the technical anonymity protections necessary to protect the identity of the source.

Perceptions of Online Reporting Systems

The results of the test of proposed system features show that certain aspects of online reporting systems do influence user perceptions of anonymity protection. Specifically, a web browser configured to use Tor, end-to-end data encryption, and the automatic removal of document meta-data significantly impacted opinions regarding the system's ability to protect user anonymity. However, the method of development and use of a system-generated passphrase did not resonate with the participants. This outcome is understandable given that most users are likely unfamiliar with how either feature would improve anonymity. Therefore, more education needs to be provided to ensure that users understand exactly how each feature can better protect their anonymity.

Implications for Practice

The purpose of this study was to assess the proposed system features from the perspective of the common user. The results show that most users are capable of recognizing the benefits of familiar features, but struggle to understand the more

technical aspects of the system. This provides system designers with insight for educating users to ensure that they fully understand the capabilities of the system.

Contributions to the Literature

This study has addressed critical gaps in the existing literature. First, the study is the first to assess user perceptions of multiple reporting channels simultaneously. Second, the study has examined user perceptions of a modern, anonymous, two-way, ethics management reporting system. Third, the study has demonstrated that the proposed system is perceived to better protect user anonymity.

Suggestions for Future Research

Future studies should consist of a replication of the system features experiment, with the addition of detailed explanations of each feature prior to assessing the system. This would aid in the goal of increasing adoption by determining effective methods for educating users on the technical aspects of the system.

Limitations

Although the study is limited by the sensitive nature of the subject matter, the use of Amazon Mechanical Turk and an anonymous, online instrument provides a safer environment for participants to provide honest responses. Further, the study involves the assessment of intentions, rather than observed behavior. Unfortunately, the nature of this topic is not conducive to such a study.

Conclusion

This study has identified, measured and analyzed the influence of various aspects of reporting channels. Specifically, three common reporting channels were compared and

the primary features of a modern design of an anonymous, two-way ethics management system were evaluated. The results have shown that online systems are perceived as offering better anonymity protection and that the proposed system features can further strengthen such beliefs.

CHAPTER FIVE

CONCLUSION

This dissertation has outlined and evaluated the necessary requirements for an anonymous, ethics management reporting system capable of maintaining two-way communication. In Chapter 2, design science (Hevner et al., 2004; March & Smith, 1995; Walls, Widmeyer, & El Sawy, 1992, 2004) was employed in order to theorize and justify the design of an anonymous reporting system artifact. In doing so, existing reporting systems were examined and modern technologies were incorporated into a proposed design of an anonymous, two-way ethics management reporting system. Constructs were built, models were developed and methods were explained in order to achieve a design which satisfies the desired goals of reporting for all actors involved.

Chapter 3 reviewed existing theories in the extant whistleblowing literature and relied upon communication research, both inter-personal and computer-mediated, to address the limitations of prior theory regarding reduced perceptions of credibility for anonymous whistleblowers. In order to assess these perceptions, investigators were solicited from a number of professional organizations to participate in an online experiment. The experiment tasked subjects with evaluating simulated two-way communication between an investigator and an employee attempting to blow the whistle on financial wrongdoing. The results of the study provide strong evidence supporting the

efficacy of two-way communication in reducing the credibility gap theorized to exist between perceptions of anonymous and identified whistleblowers, which strengthens the argument for anonymous reporting.

Lastly, Chapter 4 assessed the proposed design in Chapter 2 from the perspective of those who are likely to observe wrongdoing; that is, the organizational insider. In order to conduct a comprehensive assessment of the design, the proposed system was also compared to other reporting channels available to report wrongdoing, such as the use of open door policies and telephone hotlines. Two online experiments were conducted simultaneously in order to test user perceptions of anonymity protections provided by each channel, as well as the specific whistleblower-oriented design features proposed in the design. This chapter provides evidence that online reporting systems are perceived to provide significantly higher anonymity protections than phone hotlines and open door policies, while select features of the proposed system impact user perceptions of anonymity.

Implications for Practice

This research has a number of practical implications. Chapter 2 addressed the critical need for the design of an anonymous ethics management system and includes the addition of two-way communication capabilities between an anonymous whistleblower and investigator. As was shown in Chapter 3, this technological advancement has the potential to bridge the perceived credibility gap between anonymous and identified whistleblower reports. Addressing this issue has tremendous implications for practice in that unethical or illegal behavior reported by anonymous sources via two-way communication should receive greater consideration by investigators.

Further, the ability to protect anonymity at the system level is the best method for dramatically reducing the incidence of whistleblower retaliation. Therefore, the development of a system that is perceived by potential whistleblowers as providing the highest degree of anonymity protection, as was shown in Chapter 4, provides organizations with a more effective method of soliciting information regarding wrongdoing within the organization. Any subsequent increase in reporting as a result of implementing a system consistent with the proposed design will provide greater insight into potential problems within the organization, which allows for the appropriate corrective action to be implemented earlier.

Lastly, Chapter 4 assessed a select number of the proposed system features from the perspective of the common user. The results of this study have shown that most users are capable of recognizing the benefits of familiar features, but struggle to understand the more technical aspects of the system. This provides system designers with insight for educating users to ensure that they fully understand the capabilities of the system.

Academic Contributions

In terms of academic contributions, this research has addressed critical issues with prior theory and sets the stage for an extensive research stream in information systems. The addition of two-way communication capabilities between an anonymous whistleblower and investigator had yet to be suggested as a possibility in the extant whistleblowing literature. By suggesting this capability in Chapters 1 and 2, and testing it in Chapter 3, this research has shown that the long-held belief that anonymous whistleblowers are always perceived as less credible simply due to being anonymous is only limited to one-way communication. As was shown, investigators are just as capable

of perceiving an anonymous source to be equally as credible as an identified source when information is exchanged via two-way communication. Lastly, Chapter 4 is the first study to assess user perceptions of multiple reporting channels simultaneously, including user perceptions of a modern, anonymous, two-way, ethics management reporting system. This study has demonstrated that the proposed system is perceived as providing significantly better protection in terms of user anonymity.

Future Research

This study also leads to a number of future research directions. First, the proposed system design provides the first conceptualization of such a system in the academic literature. Although whistleblowing has been widely studied in disciplines such as management, accounting and ethics, little research has been conducted with respect to the technological aspects of this phenomenon. Therefore, this study provides an excellent foundation to propel whistleblowing research into areas of information systems research, such as computer-mediated communication, information security, and design science.

Second, since the study conducted in Chapter 3 was able to reject a number of rival explanations, simplified replications of this study can be extended to examine a wide variety of aspects which may impact investigators' perceived credibility and resource allocation, such as: (1) the seriousness of the alleged wrongdoing, (2) the various components of a whistleblowing report, and (3) whether the report is made internally or externally. Further, rather than rely upon simulated communication, experiments with active participants serving the role of both whistleblower and investigator can be conducted to examine actual dialogue in order to gain a richer picture of such communication. The investigatory resource allocation trade-off decision can also

be extended to a within-subjects experiment which requires investigators to examine and simultaneously consider multiple reports of alleged wrongdoing. This would better represent a real-world situation for the investigator as he or she would be forced to allocate limited resources to investigate potential wrongdoing, which strengthens the generalizability of this research stream.

Third, future studies could consist of a replication of the system features experiment conducted in Chapter 4, with the addition of manipulated explanations of each feature prior to assessing the system. This would aid in the goal of increasing adoption by determining effective methods for educating users on the technical aspects of the system.

Lastly, this entire research stream can be directed towards avenues in information security by advocating the use of ethics management reporting systems to assist in the identification of vulnerabilities in an organization's policies, procedures and systems. In doing so, it can be argued that organizational insiders might be more likely to engage in protection-motivation behaviors and report suspicious activity if an anonymous channel designated to receive reports of such threats is available.

APPENDIX A

HUMAN USE APPROVAL LETTER (HUC 1296)



LOUISIANA TECH
UNIVERSITY

MEMORANDUM

OFFICE OF UNIVERSITY RESEARCH

TO: Dr. Jim Courtney, Dr. Rebecca Bennett and Mr. Jacob Young
 FROM: Dr. Stan Nappor, Vice President Research & Development
 SUBJECT: HUMAN USE COMMITTEE REVIEW
 DATE: April 13, 2015

In order to facilitate your project, an EXPEDITED REVIEW has been done for your proposed study entitled:

"Examining Investigators' Perception of Reports of Wrongdoing"

HUC 1296

The proposed study's revised procedures were found to provide reasonable and adequate safeguards against possible risks involving human subjects. The information to be collected may be personal in nature or implication. Therefore, diligent care needs to be taken to protect the privacy of the participants and to assure that the data are kept confidential. Informed consent is a critical part of the research process. The subjects must be informed that their participation is voluntary. It is important that consent materials be presented in a language understandable to every participant. If you have participants in your study whose first language is not English, be sure that informed consent materials are adequately explained or translated. Since your reviewed project appears to do no damage to the participants, the Human Use Committee grants approval of the involvement of human subjects as outlined.

Projects should be renewed annually. *This approval was finalized on April 13, 2015 and this project will need to receive a continuation review by the IRB if the project, including data analysis, continues beyond April 13, 2016.* Any discrepancies in procedure or changes that have been made including approved changes should be noted in the review application. Projects involving NIH funds require annual education training to be documented. For more information regarding this, contact the Office of University Research.

You are requested to maintain written records of your procedures, data collected, and subjects involved. These records will need to be available upon request during the conduct of the study and retained by the university for three years after the conclusion of the study. If changes occur in recruiting of subjects, informed consent process or in your research protocol, or if unanticipated problems should arise it is the Researchers responsibility to notify the Office of Research or IRB in writing. The project should be discontinued until modifications can be reviewed and approved.

If you have any questions, please contact Dr. Dr. Mary Livingston at 257-2292 or 257-5066.

A MEMBER OF THE UNIVERSITY OF LOUISIANA SYSTEM

P.O. BOX 1342 • BOSSIERE, LA 71272 • TEL: (504) 257-5075 • FAX: (504) 257-4147

WWW.LOUISIANATECH.EDU

APPENDIX B

HUMAN USE APPROVAL LETTER (HUC 1323)



LOUISIANA TECH
UNIVERSITY

MEMORANDUM

OFFICE OF UNIVERSITY RESEARCH

TO: Mr. Jacob Young, Dr. Jim Courtney and Dr. Rebecca Bennett
 FROM: Dr. Stan Napper, Vice President Research & Development
 SUBJECT: HUMAN USE COMMITTEE REVIEW
 DATE: May 28, 2015

In order to facilitate your project, an EXPEDITED REVIEW has been done for your proposed study entitled:

"Drivers in the Adoption of Ethics Management Reporting Channels"

HUC 1323

The proposed study's revised procedures were found to provide reasonable and adequate safeguards against possible risks involving human subjects. The information to be collected may be personal in nature or implication. Therefore, diligent care needs to be taken to protect the privacy of the participants and to assure that the data are kept confidential. Informed consent is a critical part of the research process. The subjects must be informed that their participation is voluntary. It is important that consent materials be presented in a language understandable to every participant. If you have participants in your study whose first language is not English, be sure that informed consent materials are adequately explained or translated. Since your reviewed project appears to do no damage to the participants, the Human Use Committee grants approval of the involvement of human subjects as outlined.

Projects should be renewed annually. *This approval was finalized on May 28, 2015 and this project will need to receive a continuation review by the IRB if the project, including data analysis, continues beyond May 28, 2016.* Any discrepancies in procedure or changes that have been made including approved changes should be noted in the review application. Projects involving NIH funds require annual education training to be documented. For more information regarding this, contact the Office of University Research.

You are requested to maintain written records of your procedures, data collected, and subjects involved. These records will need to be available upon request during the conduct of the study and retained by the university for three years after the conclusion of the study. If changes occur in recruiting of subjects, informed consent process or in your research protocol, or if unanticipated problems should arise it is the Researcher's responsibility to notify the Office of Research or IRB in writing. The project should be discontinued until modifications can be reviewed and approved.

If you have any questions, please contact Dr. Di. Mary Livingston at 257-2292 or 257-5066.

A MEMBER OF THE UNIVERSITY OF LOUISIANA SYSTEM

PO BOX 2272 • RUSSELL, LA 72724 • TEL: (257) 257-2272 • FAX: (257) 257-2272

A COMMITMENT TO EXCELLENCE

REFERENCES

- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40–46. doi:10.1145/322796.322806
- Adler, P. S., & Kwon, S.-W. (2002). Social capital: Prospects for a new concept. *Academy of Management Review*, 27(1), 17–40.
- Alford, C. F. (2001). *Whistleblowers: Broken Lives and Organizational Power* (First Edit.). Ithaca, New York: Cornell University Press.
- Ashford, S., Rothbard, N., Piderit, S. K., & Dutton, J. E. (1998). Out on a limb: The role of context and impression management in selling gender-equity issues. *Administrative Science Quarterly*, 43(1), 23–57.
- Ashforth, B. E., & Mael, F. (1989). Social identity theory and the organization. *Academy of Management Review*, 14(1), 20–39.
- Ayers, S., & Kaplan, S. E. (2005). Wrongdoing by Consultants: An Examination of Employees' Reporting Intentions. *Journal of Business Ethics*, 57(2), 121–137. doi:10.1007/s10551-004-4600-0
- Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological Antecedents and Implications. *MIS Quarterly*, 35(4), 831. Retrieved from <http://search.proquest.com/docview/906375245?accountid=14570>
- Bamberger, K. (2006). Regulation as delegation: Private firms, decisionmaking, and accountability in the administrative state. *Duke Law Journal*, 56(2), 337–468.
- Barnett, T., Cochran, D. S., & Taylor, G. S. (1993). The internal disclosure policies of private-sector employers: An initial look at their relationship to employee whistleblowing. *Journal of Business Ethics*, 12(2), 127–136. doi:10.1007/BF00871932
- Barnlund, D. C. (1970). A Transactional Model of Communication. In *Language Behavior: A Book of Readings in Communication* (pp. 43–61).
- Behrend, T. S., Sharek, D. J., Meade, A. W., & Wiebe, E. N. (2011). The viability of crowdsourcing for survey research. *Behavior Research Methods*, 43(3), 800–813. doi:10.3758/s13428-011-0081-0

- Berlo, D. (1960). *Process of Communication: An Introduction to Theory and Practice*. Harcourt School.
- Biermann, K. (2011, March 26). Data Protection: Betrayed by our own data. *Die Zeit Online*. Hamburg, Germany. Retrieved from <http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz>
- Bjørkelo, B., Bye, H. H., & Bj, B. (2014). On the appropriateness of research design: Intended and actual whistleblowing. In A. J. Brown, D. Lewis, R. E. Moberly, & W. Vandekerckhove (Eds.), *International Handbook on Whistleblowing Research* (pp. 133–153). Cheltenham, UK: Edward Elgar Publishing. doi:10.4337/9781781006795.00013
- Bowie, N. (1982). *Business Ethics*. Englewood Cliffs, NJ: Prentice-Hall.
- Buhrmester, M. D., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data? *Perspectives on Psychological Science*, 6(1), 3–5. doi:10.1177/1745691610393980
- Callahan, E. S., & Dworkin, T. M. (1992). Do Good and Get Rich: Financial Incentives for Whistleblowing and the False Claims Act. *Villanova Law Review*, 37(2), 273–336.
- Callahan, E. S., Dworkin, T. M., Fort, T. L., & Schipani, C. A. (2002). Integrating Trends in Whistleblowing and Corporate Governance: Promoting Organizational Effectiveness, Societal Responsibility, and Employee Empowerment. *American Business Law Journal*, 40(1), 177–215. doi:10.1111/j.1744-1714.2002.tb00913.x
- Casler, K., Bickel, L., & Hackett, E. (2013). Separate but equal? A comparison of participants and data gathered via Amazon's MTurk, social media, and face-to-face behavioral testing. *Computers in Human Behavior*, 29(6), 2156–2160. doi:10.1016/j.chb.2013.05.009
- Chen, C., Asoni, D. E., Barrera, D., Danezis, G., & Perrig, A. (2015). HORNET: High-speed Onion Routing at the Network Layer. Retrieved from <http://arxiv.org/abs/1507.05724>
- Cheng, H. K., Liu, Y., & Tang, Q. (Candy). (2011). The Impact of Network Externalities on the Competition Between Open Source and Proprietary Software. *Journal of Management Information Systems*, 27(4), 201–230. doi:10.2753/MIS0742-1222270407
- Daft, R. L., & Lengel, R. H. (1984). Information richness: a new approach to managerial behavior and organizational design. In B. M. Staw & L. L. Cummings (Eds.), *Research in Organizational Behavior* (pp. 191–233). Homewood, IL: JAI Press Inc.
- DeGeorge, R. T. (1986). *Business Ethics*. New York, NY: MacMillan.

- Detert, J. R., & Burris, E. R. (2007). Leadership Behavior and Employee Voice: Is the Door Really Open? *Academy of Management Journal*, 50(4), 869–884. doi:10.5465/AMJ.2007.26279183
- Detert, J. R., & Trevino, L. K. (2010). Speaking Up to Higher-Ups: How Supervisors and Skip-Level Leaders Influence Employee Voice. *Organization Science*, 21(1), 249–270. doi:10.1287/orsc.1080.0405
- Devine, T., & Maassarani, T. F. (2011). *The Corporate Whistleblower's Survival Guide*. San Francisco, CA: Berrett-Koehler Publishers, Inc.
- Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.
- Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111-203, 124 Stat. 1376. United States.
- Dworkin, T. M., & Baucus, M. S. (1998). Internal vs. External Whistleblowers: A Comparison of Whistleblowing Processes. *Journal of Business Ethics*, 17(12), 1281–1298. doi:10.1023/A:1005916210589
- Dyck, A., Morse, A., & Zingales, L. (2010). Who Blows the Whistle on Corporate Fraud? *The Journal of Finance*, LXV(6), 2213–2253.
- Elias, R. (2008). Auditing students' professional commitment and anticipatory socialization and their relationship to whistleblowing. *Managerial Auditing Journal*, 23(3), 283–294. doi:10.1108/02686900810857721
- Elliston, F. A. (1981). Anonymous Whistleblowing: An Ethical Analysis. *Business & Professional Ethics Journal*, 1(2), 39–59.
- Elliston, F. A. (1982). Anonymity and whistleblowing. *Journal of Business Ethics*, 1(3), 167–177. doi:10.1007/BF00382768
- Ethics Resource Center. (2010). *Blowing the Whistle on Workplace Misconduct*. Arlington, VA.
- Ethics Resource Center. (2013). *National Business Ethics Survey of the U.S. Workforce*. Arlington, Virginia.
- Free Software Foundation. (2015, September 1). The Free Software Definition. Retrieved September 6, 2015, from <http://www.gnu.org/philosophy/free-sw.en.html>
- Fuller, C. M., Biros, D. P., & Delen, D. (2011). An investigation of data and text mining methods for real world deception detection. *Expert Systems with Applications*, 38(7), 8392–8398. doi:10.1016/j.eswa.2011.01.032

- Fuller, C. M., Biros, D. P., & Wilson, R. L. (2009). Decision support for determining veracity via linguistic-based cues. *Decision Support Systems*, 46(3), 695–703. doi:10.1016/j.dss.2008.11.001
- Goldschlag, D., Reed, M., & Syverson, P. (1996). Hiding Routing Information. In *Workshop on Information Hiding* (Vol. 1174, pp. 137–150). Cambridge, UK. doi:10.1007/3-540-61996-8_37
- Green, M. (2004, January). How's My Accounting? *Best's Review*, 104(9), 66. Retrieved from <http://search.proquest.com/docview/205507785?accountid=14549&http://hl5yy6xn2p.search.serialssolutions.com/?genre=article&sid=ProQ:&atitle=How's+My+Accounting?&title=Best's+Review&issn=15275914&date=2004-01-01&volume=104&issue=9&spage=66&author=Green,+Me>
- Hair, J. F., Black, B., Babin, B., Anderson, R. E., & Tatham, R. L. (2005). *Multivariate Data Analysis* (6th ed.). Upper Saddle River, New Jersey: Prentice Hall.
- Hassink, H., Vries, M., & Bollen, L. (2007). A Content Analysis of Whistleblowing Policies of Leading European Companies. *Journal of Business Ethics*, 75(1), 25–44. doi:10.1007/s10551-006-9236-9
- Hayashi, E., & Hong, J. I. (2011). A diary study of password usage in daily life. *Analysis*, 2627–2630. doi:10.1145/1978942.1979326
- Hellman, M. E. (2002). An overview of public key cryptography. *IEEE Communications Magazine*, 40(5), 42–49. doi:10.1109/MCOM.2002.1006971
- Hevner, A. R., March, S. T., Park, J., Ram, S., Esearch, S. Y. R., Hevner, B. A. R., ... Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75–105. Retrieved from <http://dl.acm.org/citation.cfm?id=2017212.2017217>
- Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, 47(4), 75–78. doi:10.1145/975817.975820
- Jackson, D., Peters, K., Andrew, S., Edenborough, M., Halcomb, E., Luck, L., ... Wilkes, L. (2010). Understanding whistleblowing: qualitative insights from nurse whistleblowers. *Journal of Advanced Nursing*, 66(10), 2194–201. doi:10.1111/j.1365-2648.2010.05365.x
- Jessup, L. M., & Tansik, D. A. (1991). Decision Making in an Automated Environment: The Effects of Anonymity and Proximity with a Group Decision Support System. *Decision Sciences*, 22(2), 266–279. doi:10.1111/j.1540-5915.1991.tb00346.x
- Jones, D. (2003, May 27). Law rings up growth in worker hotline industry. *USA Today*, pp. Money, 3b.

- Jos, P. H., Tompkins, M. E., & Hays, S. W. (1989). In Praise of Difficult People: A Portrait of the Committed Whistleblower. *Public Administration Review*, 49(6), 552–561. doi:10.2307/976577
- Kahn, D. (1996). *The Code-Breakers: The Story of Secret Writing*. New York, New York: Scribner.
- Kalman, Y. M., & Rafaeli, S. (2011). Online Pauses and Silence: Chronemic Expectancy Violations in Written Computer-Mediated Communication. *Communication Research*, 38(1), 54–69. doi:10.1177/0093650210378229
- Kaplan, S. E., & Schultz, J. (2006). *The role of internal audit in sensitive communications*. Altamonte Springs, FL.
- Kaplan, S. E., & Schultz, J. J. (2007). Intentions to Report Questionable Acts: An Examination of the Influence of Anonymous Reporting Channel, Internal Audit Quality, and Setting. *Journal of Business Ethics*, 71(2), 109–124. doi:10.1007/s10551-006-0021-6
- Kaptein, M. (2002). Guidelines for the development of an ethics safety net. *Journal of Business Ethics*, 41(3), 217–234. doi:10.1023/A:1021221211283
- Kaptein, M. (2010). From Inaction to External Whistleblowing: The Influence of the Ethical Culture of Organizations on Employee Responses to Observed Wrongdoing. *Journal of Business Ethics*, 98(3), 513–530. doi:10.1007/s10551-010-0591-1
- Karpoff, J., Lee, D., & Martin, G. (2008). The Cost to Firms of Cooking the Books. *Journal of Financial and Quantitative Analysis*, 43(3), 581–612.
- Kerckhoffs, A. (1883). La cryptographie militaire. *Journal Des Sciences Militaires*, IX, 5–38. Retrieved from <http://www.petitcolas.net/fabien/kerckhoffs/>
- Knoll, M., & van Dick, R. (2013). Do I Hear the Whistle...? A First Attempt to Measure Four Forms of Employee Silence and Their Correlates. *Journal of Business Ethics*, 113(2), 349–362. doi:10.1007/s10551-012-1308-4
- Kohn, S. M. (2011). *The Whistleblower's Handbook: A Step-by-Step Guide to Doing What's Right and Protecting Yourself*. Guilford, Connecticut: Lyons Press.
- Landau, S. (2013). Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. *IEEE Security & Privacy*, 11(4), 54–63. doi:10.1109/MSP.2013.90
- Landau, S. (2014). Highlights from making Sense of Snowden, Part II: What's significant in the NSA revelations. *IEEE Security and Privacy*, 12(1), 62–64. doi:10.1109/MSP.2013.161

- Larmer, R. A. (1992). Whistleblowing and employee loyalty. *Journal of Business Ethics*, 11(2), 125–128. doi:10.1007/BF00872319
- Lerner, J., & Tirole, J. (2003). Some Simple Economics of Open Source. *The Journal of Industrial Economics*, 50(2), 197–234. doi:10.1111/1467-6451.00174
- Levene, H. (1960). Robust Tests for Equality of Variances. In I. Olkin (Ed.), *Contributions to Probability and Statistics* (pp. 278–292). Palo Alto, California: Stanford University Press.
- Liang, J., Farh, C., & Farh, J. (2012). Psychological antecedents of promotive and prohibitive voice: A two-wave examination. *Academy of Management Journal*, 55(1), 71–92.
- Liyanarachchi, G., & Newdick, C. (2008). The Impact of Moral Reasoning and Retaliation on Whistle-Blowing: New Zealand Evidence. *Journal of Business Ethics*, 89(1), 37–57. doi:10.1007/s10551-008-9983-x
- Lowry, P. B., Moody, G. D., Galletta, D. F., & Vance, A. (2013). The Drivers in the Use of Online Whistle-Blowing Reporting Systems. *Journal of Management Information Systems*, 30(1), 153–190. doi:10.2753/MIS0742-1222300105
- MacNab, B. R., Brislin, R., Worthley, R., Galperin, B. L., Jenner, S., Lituchy, T. R., ... Turcotte, M.-F. (2007). Culture and Ethics Management: Whistle-blowing and Internal Reporting within a NAFTA Country Context. *International Journal of Cross Cultural Management*, 7(1), 5–28. doi:10.1177/1470595807075167
- MacNab, B. R., & Worthley, R. (2007). Self-Efficacy as an Intrapersonal Predictor for Internal Whistleblowing: A US and Canada Examination. *Journal of Business Ethics*, 79(4), 407–421. doi:10.1007/s10551-007-9407-3
- March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, 15(4), 251–266. doi:10.1016/0167-9236(94)00041-2
- McMahon, J. M., & Harvey, R. J. (2006). An Analysis of the Factor Structure of Jones' Moral Intensity Construct. *Journal of Business Ethics*, 64(4), 381–404. doi:10.1007/s10551-006-0006-5
- Merkle, R. C. (1978). Secure Communications Over Insecure Channels. *Communications of the ACM*, 21(4), 294–299. doi:10.1145/359460.359473
- Merriam-Webster. (n.d.). Anonymity. In *Merriam-Webster*. Retrieved from <http://www.merriam-webster.com/dictionary/anonymity>
- Mesmer-Magnus, J. R., & Viswesvaran, C. (2005). Whistleblowing in Organizations: An Examination of Correlates of Whistleblowing Intentions, Actions, and Retaliation. *Journal of Business Ethics*, 62(3), 277–297. doi:10.1007/s10551-005-0849-1

- Miceli, M. P., & Near, J. P. (1985). Characteristics of Organizational Climate and Perceived Wrongdoing Associated With Whistle-Blowing Decisions. *Personnel Psychology*, 38(3), 525–544. doi:10.1111/j.1744-6570.1985.tb00558.x
- Miceli, M. P., & Near, J. P. (1992). *Blowing the Whistle: The Organizational & Legal Implications for Companies and Employees*. New York, NY: Lexington Books.
- Miceli, M. P., & Near, J. P. (1994). Whistleblowing: Reaping the benefits. *Academy of Management Perspectives*, 8(3), 65–72. doi:10.5465/AME.1994.9503101177
- Miceli, M. P., & Near, J. P. (2005). Standing up or standing by: What predicts blowing the whistle on organizational wrongdoing? In J. J. Martocchio (Ed.), *Research in Personnel and Human Resources Management* (pp. 95–136). Emerald Group Publishing Limited. doi:10.1016/S0742-7301(05)24003-3
- Miceli, M. P., & Near, J. P. (2013). Some implications of the voice literature for research on whistle-blowing. In R. J. Burke & C. L. Cooper (Eds.), *Voice and Whistleblowing in Organizations* (pp. 182–202). Cheltenham, UK: Edward Elgar Publishing Limited. doi:10.4337/9781781005927.00016
- Miceli, M. P., Near, J. P., & Dworkin, T. M. (2008a). A Word to the Wise: How Managers and Policy-Makers can Encourage Employees to Report Wrongdoing. *Journal of Business Ethics*, 86(3), 379–396. doi:10.1007/s10551-008-9853-6
- Miceli, M. P., Near, J. P., & Dworkin, T. M. (2008b). *Whistle-Blowing in Organizations*. New York, NY: Routledge.
- Morrison, E., & Milliken, F. (2000). Organizational silence: A barrier to change and development in a pluralistic world. *Academy of Management Review*, 25(4), 706–725.
- National Computer Security Center. (1991, September 1). NCSC-TG-017: A Guide to Understanding Identification and Authentication in Trusted Systems.
- Near, J. P. (1989). Whistle-Blowing: Encourage It! *Business Horizons*, 32(1), 2–6.
- Near, J. P., & Jensen, T. C. (1983). The Whistleblowing Process: Retaliation and Perceived Effectiveness. *Work and Occupations*, 10(1), 3–28. doi:10.1177/0730888483010001001
- Near, J. P., & Miceli, M. P. (1986). Retaliation against whistle blowers: Predictors and effects. *Journal of Applied Psychology*, 71(1), 137–145. doi:10.1037/0021-9010.71.1.137
- Near, J. P., & Miceli, M. P. (1995). Effective-Whistle Blowing. *Academy of Management Review*, 20(3), 679–708. doi:10.5465/AMR.1995.9508080334

- Near, J. P., & Miceli, M. P. (1996). Whistle-blowing: Myth and reality. *Journal of Management*, 22(3), 507–526. doi:10.1177/014920639602200306
- Near, J. P., Rehg, M. T., Van Scotter, J. R., & Miceli, M. P. (2004). Does type of wrongdoing affect the whistle-blowing process? *Business Ethics Quarterly*, 14(2), 219–242. Retrieved from <http://www.jstor.org/stable/10.2307/3857908>
- Olsen, J. (2014). Reporting versus inaction: How much is there, what explains the differences and what to measure. In A. J. Brown, D. Lewis, R. E. Moberly, & W. Vandekerckhove (Eds.), *International Handbook on Whistleblowing Research* (pp. 177–206). Edward Elgar Publishing. doi:10.4337/9781781006795.00016
- Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on amazon mechanical turk. *Judgment and Decision Making*, 5(5), 411–419. Retrieved from <http://repub.eur.nl/pub/31983>
- Park, C., & Keil, M. (2009). Organizational Silence and Whistle-Blowing on IT Projects: An Integrated Model. *Decision Sciences*, 40(4), 901–918. doi:10.1111/j.1540-5915.2009.00255.x
- Park, H., & Blenkinsopp, J. (2008). Whistleblowing as Planned Behavior – A Survey of South Korean Police Officers. *Journal of Business Ethics*, 85(4), 545–556. doi:10.1007/s10551-008-9788-y
- Penman, C., & O'Mara, E. (2014). *2014 Hotline Benchmarking Report*.
- Pfutzmann, A., & Hansen, M. (2010). *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management* (No. v0.34). Retrieved from <http://staging.kantarinitiative.org/confluence/download/attachments/45059055/terminology+for+talking+about+privacy.pdf>
- Pinder, C. C., & Harlos, K. P. (2001). Employee silence: Quiescence and acquiescence as responses to perceived injustice. In M. Buckley, J. Halbesleben, & A. R. Wheeler (Eds.), *Research in Personnel and Human Resources Management* (20th ed., Vol. 20, pp. 331–369). Emerald Group Publishing Limited. doi:10.1016/S0742-7301(01)20007-3
- Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' Protection of Organizational Information Assets: Development of a Systematics-based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors. *MIS Quarterly*, 37(4), 1189–1210.
- Rigby, P., Cleary, B., Painchaud, F., Storey, M.-A., & German, D. (2012). Contemporary Peer Review in Action: Lessons from Open Source Development. *IEEE Software*, 29(6), 56–61. doi:10.1109/MS.2012.24

- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2), 120–126. Retrieved from <http://dl.acm.org/citation.cfm?id=359342>
- Rosen, S., & Tesser, A. (1970). On Reluctance to Communicate Undesirable Information: The MUM Effect. *Sociometry*, 33(3), 253. doi:10.2307/2786156
- Rothschild, J., & Miethe, T. D. (1999). Whistle-Blower Disclosures and Management Retaliation: The Battle to Control Information about Organization Corruption. *Work and Occupations*, 26(1), 107–128. doi:10.1177/0730888499026001006
- Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745. 107th U.S. Congress.
- Schnatterly, K. (2003). Increasing firm value through detection and prevention of white-collar crime. *Strategic Management Journal*, 24(7), 587–614. doi:10.1002/smj.330
- Shafer, W. (2002). Effects of Materiality, Risk, and Ethical Perceptions on Fraudulent Reporting by Financial Executives. *Journal of Business Ethics*, 38(3), 243–262. doi:10.1023/A:1016049022458
- Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technology Journal*, 27(July 1928), 379–423, 623–656. doi:10.1145/584091.584093
- Sherwood, R., Bhattacharjee, B., & Srinivasan, A. (2005). P5: A protocol for scalable anonymous communication. *Journal of Computer Security*, 13(6), 839–876.
- Silowash, G. J., Cappelli, D. M., Moore, A., Trzeciak, R. F., Shimeall, T. J., & Flynn, L. (2012). *Common Sense Guide to Mitigating Insider Threats*.
- Simon, H. A. (1988). The Science of Design: Creating the Artificial. *Designing the Immaterial Society*, 4(1/2), 67–82.
- Sims, R. R. L., & Keenan, J. P. (1998). Predictors of external whistleblowing: Organizational and intrapersonal variables. *Journal of Business Ethics*, 17(4), 411–421. doi:10.1023/A:1005763807868
- Smith, H. J., & Keil, M. (2003). The reluctance to report bad news on troubled software projects: a theoretical model. *Information Systems Journal*, 13(1), 69–95. doi:10.1046/j.1365-2575.2003.00139.x
- Smith, K., & Oseth, J. (1993). The Whistleblowing Era: A Management Perspective. *Employee Relations Law Journal*, 19(2), 179–192.
- Tangirala, S., & Ramanujam, R. (2008). Employee Silence on Critical Work Issues: The Cross Level Effects of Procedural Justice Climate. *Personnel Psychology*, 61(1), 37–68. doi:10.1111/j.1744-6570.2008.00105.x

- Tell-all telephone. (2011). *Die Zeit Online*. Retrieved July 16, 2015, from <http://www.zeit.de/datenschutz/malte-spitz-data-retention/>
- The Amnesic Incognito Live System. (2015, May 16). Design: specification and implementation. Retrieved September 6, 2015, from <https://tails.boum.org/contribute/design/>
- The Tor Project. (2015a). Tor: Hidden Service Protocol. Retrieved September 8, 2015, from <https://www.torproject.org/docs/hidden-services.html.en>
- The Tor Project. (2015b). Tor: Overview. Retrieved September 8, 2015, from <https://www.torproject.org/about/overview.html.en>
- U.S. Federal Communications Commission. (2014a). Wireline Competition Bureau Data and Statistical Reports. *FCC Encyclopedia*. Washington, D.C. Retrieved from <https://www.fcc.gov/encyclopedia/statistical-reports-telephone-and-broadband-services>
- U.S. Federal Communications Commission. (2014b). Wireline Competition Bureau Data and Statistical Reports. *FCC Encyclopedia*. Washington, D.C.
- U.S. Securities and Exchange Commission. (2013, October 1). SEC Awards More Than \$14 Million to Whistleblower. Washington, D.C.: U.S. Securities and Exchange Commission. Retrieved from <http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539854258>
- U.S. Securities and Exchange Commission. (2014, September 22). SEC Announces Largest-Ever Whistleblower Award. Washington, D.C.: U.S. Securities and Exchange Commission. Retrieved from <http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543011290>
- U.S. Securities and Exchange Commission. (2015, April 28). SEC Announces Award to Whistleblower in First Retaliation Case. Washington, D.C. Retrieved from <http://www.sec.gov/news/pressrelease/2015-75.html>
- Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance and Society*, 12(2), 197–208.
- Van Dyne, L., Ang, S., & Botero, I. C. (2003). Conceptualizing Employee Silence and Employee Voice as Multidimensional Constructs. *Journal of Management Studies*, 40(6), 1359–1392. doi:10.1111/1467-6486.00384
- Vandekerckhove, W., Uys, T., Rehg, M. T., & Brown, A. J. (2014). Understandings of whistleblowing: Dilemmas of societal culture. In A. J. Brown, D. Lewis, R. E. Moberly, & W. Vandekerckhove (Eds.), *International Handbook on Whistleblowing Research* (pp. 37–70). Edward Elgar Publishing. doi:10.4337/9781781006795.00009

- Velasquez, M. G. (2005). *Business Ethics: Concepts & Cases* (6th ed.). New York, NY: Prentice Hall.
- Von Krogh, G., Haefliger, S., Spaeth, S., & Wallin, M. W. (2012). Carrots and Rainbows: Motivation and Social Practice in Open Source Software Development. *MIS Quarterly*, 36(2), 649–676. Retrieved from <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=74756698&site=ehost-live\nhttp://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=74756698&S=R&D=buh&EbscoContent=dGJyMMTo50SeprY4zOX0OLCmr0ueprNSr6u4SbOWxWXS&ContentCustomer=dGJyMPGok+xrLZQu>
- Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an Information System Design Theory for Vigilant EIS. *Information Systems Research*, 3(1), 36–59. doi:10.1287/isre.3.1.36
- Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (2004). Assessing Information System Design Theory in Perspective: How Useful was our 1992 Initial Rendition? *Journal of Information Technology Theory and Application*, 6(2), 43–58. Retrieved from http://iris.nyit.edu/~kkhoo/Spring2008/Topics/DS/DtheoryAssessing_JITTA2004.pdf
- Wang, J., Keil, M., & Wang, L. I. (2015). The Effect of Moral Intensity on IT Employees' Bad News Reporting. *Journal of Computer Information Systems*, 55(3), 1–10.
- Weaver, G., Trevino, L. K., & Cochran, P. (1999). Corporate ethics practices in the mid-1990's: An empirical study of the Fortune 1000. *Journal of Business Ethics*, 18(3), 283–294. doi:10.1023/A:1005726901050
- Withey, M., & Cooper, W. H. (1989). Predicting exit, voice, loyalty, and neglect. *Administrative Science Quarterly*, 34(4), 521–539.
- Young, J. R. (2006, April 21). Microsoft Word's Hidden Tags Reveal Once-Anonymous Peer Reviewers. *The Chronicle of Higher Education*, pp. A41–A42. Retrieved from <http://chronicle.com/article/Microsoft-Word-s-Hidden-Tags/16779>
- Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmeier, J. (2009). Improving multiple-password recall: an empirical study. *European Journal of Information Systems*, 18(2), 165–176. doi:10.1057/ejis.2009.9
- Zviran, M., & Haga, W. J. (1999). Password security: an empirical study. *Journal of Management Information Systems*, 15(4), 161–185. Retrieved from <http://dl.acm.org/citation.cfm?id=1189470>