

## **CASE STUDY: EXPLORATION OF HOW TECHNOLOGY AND SOCIAL MEDIA USE IS RELATED TO INTERNET PRIVACY CONCERNS IN A DIRECT SALES ORGANIZATION**

*Robert L. Totterdale, Florida Gulf Coast University, rtotterdale@fgcu.edu*

### **ABSTRACT**

*Businesses and individuals are increasingly subjected to security breaches and disclosures of personal and financial information. Additionally, as social media, mobile computing applications, and other web based software become pervasive in our daily lives, concerns about the safety and integrity of information is gaining the attention of businesses, individuals and governments on a global basis. Based on survey research of 270 salespersons, this study explores relationships between concerns about internet privacy and the utilization of technology in a global direct sales organization. Quantitative responses were assessed to understand attitudes regarding the use of technology to support sales, service, education, and communications. Statistically significant relationships between age, intention to use technology, usage frequency, and internet privacy concerns were found. The privacy paradox was also confirmed.*

**Keywords:** Internet Privacy, Information Technology (IT), Social Media, Direct Sales

### **INTRODUCTION**

This paper explores how internet privacy security concerns relate to the use of technology and social media in a global direct sales organization. Using case study methods, survey research was conducted with 270 geographically dispersed participants to gain an understanding of their attitudes toward the use of technology and their level of concerns relating to internet privacy; both from their perspective and the perspective of their customers. Provided in the following sections are overviews of the direct sales industry and the characteristics of the organization chosen for this research, a discussion of internet privacy and security concerns, the methods used for conducting the research, research results and conclusions.

#### **Direct Sales Industry Overview**

Direct sales is big business. The SBA [21] indicates that there are 28 million small businesses in the U.S., and that over 22m of these are self-employed individuals (with no additional payroll). In 2014, the Direct Selling Association estimated that there were 16.8m direct salespersons (self-employed) in the U.S. that accounted for over \$32b in sales of products and services (e.g. cosmetics, jewelry, clothing, candles) [7]. The age distribution of the direct sales force (which is predominately female) in the U.S. is estimated to be approximately 13.7% from age 18-29, 37% from 30-46, 34% from 47-64, and 15.3% over 65. Globally, the World Federation of Direct Selling Associations reported sales of \$178b and 96m independent sales professionals [26]. These independent direct salespersons market and sell a variety of products and services including cosmetics, apparel and accessories, home decorating items, candles, health and wellness items, as well as legal and financial services [15]. Many of these sales are conducted in one to one transactions while others are sold through home shopping parties [6]. Recent technological advances now allow for customers to place orders electronically over the internet with their direct sales representative.

The foundation of the direct selling industry is based on leveraging an individual's social networks to create successful sales opportunities [19]. Social media has substantially extended the reach of direct sales representatives through the utilization of technologies such as Facebook (personal and business), LinkedIn, YouTube, and Twitter among others [9]. Considering that over 74% of the adult population in the United States utilize Facebook for social networking, it is not surprising that both large and small businesses have embraced this technology to support business functions such as recruiting, communications, marketing, collaboration, sales, and advertising. A summary of the top five largest direct sales organizations is provided below in Table 1.

**Table 1.** Top 5 Direct Sales Organizations

2014 Rank	Company Name	2013 Revenue (\$B)
1	Amway	11.8
2	Avon	9.9
3	Herbalife	4.8
4	Vorwerk	3.7
5	Mary Kay	3.6

With respect to technology usage, Ferrell & Ferrell [8] found that 76% of direct sellers utilize social media for promotional purposes, 55% use it for recruiting, and 42% use it for reactive purposes.

### Case Company Characteristics

The company participating in this study (confidential) is a global direct sales organization with over \$1billion in annual sales and has over 500,000 direct sales representatives. Consistent with industry norms, a majority of the sales representatives are female and have a status of being independent contractors with the company. Although the sales representatives legally are contractors, they are part of a strong corporate culture and affiliate with the global direct sales organization. Organizationally, the representatives get direction and support from Directors or in some cases regional personnel, and can have representatives reporting to them. To support the representatives in the field, the organization provides product and product distribution services, high level marketing and advertising support, and technology to assist representatives in the conduct of their business. Examples of technology support include the provision of a corporate web-site for training, marketing, and branding purposes, a personal website, a CRM product that records contacts, sales, accounts receivable and cash receipts, and a strong presence in social media including Facebook, Pinterest, and YouTube, among others. The corporation also provides product and advertising content that can be linked into the representative's individual business Facebook account.

As part of the business operating model, each representative makes the choice of what (if any) of the corporate tools they will use in their business as well as any other personally selected technologies and social media tools (e.g. Facebook, business web site, Pinterest, YouTube, and LinkedIn). Consistent with the direct sales industry model, many sales are made face to face either individually or as part of parties where small groups of customers and prospective customers either see or experience the product. However, customers can now also order direct on-line from their representative's web-site and in some cases have the product direct shipped to them. A profile of the survey participants is included in Table 2.

**Table 2.** Participant Profile

Age	Count	% of total	Role	Count	% of total
Gen Y	65	24%	Director	64	24%
Gen X	69	26%	Non-Director	206	76%
Boomers	136	50%			
Income			Education		
0-2k	122	45%	High School +	118	44%
2k- 19k	59	22%	Bachelors	111	41%
20k to 49k	59	22%	Masters+	41	15%
50k+ to 200k+	30	11%			

### Internet Privacy

This research examines concerns about privacy and whether relationships exist between these concerns and how technology is used in a direct sales organization. The following sections provide an overview of privacy awareness and concerns, a definition of privacy, a review of the literature relating to privacy research, and scales that have been used to assess privacy concerns and their impacts on individuals and businesses.

## **Privacy Awareness and Legal Aspects**

Security breaches have led to the exposure of over 816m records of individuals and businesses since 2005 [18]. Companies of all sizes, including well known organizations such as eBay, Target, Experian, and Home Depot have experienced data loss that has caused privacy and financial concerns on the part of many of their customers, employees and suppliers. Industries such as retail, healthcare, financial and insurance have all seen personal account information disclosed outside of their organizations. This has led to changes in how data is secured, laws are written, and standards that address how financial/credit card information is processed. These disclosures and their reporting by the press have also raised privacy concerns by individuals and businesses that use the internet for both personal and business purposes. Although recent events have raised awareness levels, Jupiter Research in 2002 indicated that concern about internet privacy has existed for some time, with over 70% of individuals reporting concerns about privacy [3]. Given attitudes about privacy concerns, one might expect behavior to be influenced by the presence of the concerns. However, research has found a paradox in online behavior; where, although high levels of concern exist, negative behaviors regarding online use have not been observed [17].

In addition to privacy awareness, the cost of security breaches that expose personal data has also received considerable attention. During 2014, research performed by Ponemon[16], indicates that the average cost of cybercrime per research participant has risen to \$12.7m, a 9% increase over the previous year. Additionally, Ponemon estimates that the cost of cybercrime for one of the organizations in their study was over \$50m. The magnitude of costs relating to security breaches further raises the awareness of the public and organizations about privacy risk.

Lastly, legal aspects of privacy are challenging businesses as personal information becomes more vulnerable. Lawsuits against major web sites such as Google Buzz, Facebook and AOL for violation of on-line privacy regulations demonstrate the increased importance of privacy in society [10]. Laws such as HIPAA, Gramm-Leach Bliley, and the Fair Information Privacy Practices Act [11] are examples of U.S. based legislation that has been implemented that address different aspects of information privacy.

## **Internet Privacy Concerns**

Information privacy is defined by Westin [25] as the control over when, how, and to what extent information about an individual is communicated to others. While in a legal context, privacy has been considered to be the right to be left alone [24]. A number of different constructs have been developed and used in I.S. research relating to information privacy including the following;

- Global Information Privacy Concern construct; which is a single indicator of privacy concerns [20]
- Concern for Information Privacy (CFIP) construct; which is a multidimensional scale representing four dimensions including collection, unauthorized secondary use, improper access and errors [23].
- Information Privacy Situation Awareness (IPSA); which considers elements in the environment and the comprehension of their meaning [20]
- Internet Users Information Privacy Concerns (IUIPC); which considers collection, control, and awareness as three major dimensions [13] and focuses specifically on e-commerce and privacy concerns.

Research relating to information privacy has been broad addressing topics ranging from culture, trust, technologies, attitudes and E-business impacts [2]. Although several studies have used single question scales, Preibusch [17] argues that a single question instrument should be avoided and that scales by Smith and Malhorta, while mature, suffer from the absence of reverse coded items. Relating to survey instruments, Hong & Thong [10] argue that there are significant differences in the measurement of information privacy concerns where items are phrased differently from different perspectives, both within and between instruments. Another limitation of much of the existing research and related survey instruments is that it has been applied to students as opposed to groups, organizations, and societies. Privacy is typically assessed as one of several factors that may influence behaviors toward technology acceptance and adoption. Several of the survey instruments consider perceptions or expectations relating to privacy, but often do not consider both.

For research that has been completed related to the adoption of technology, privacy concerns have not been found to have a significant influence [5]. In contrast, Eastlick, Chellappa, Sin and Pavlou, have found that higher levels of concerns relating to privacy do lower intentions to use technology [2]. Privacy concerns have also been shown to have minimal impact on trust related behaviors [4]. Lastly Smith, Dinev and Xu [23] address the notion of “privacy calculus” that suggest that individuals, when considering privacy concerns, will assess the tradeoffs between costs and benefits to determine an individual’s behavioral intentions.

With substantive areas of research focused on privacy and a lack of agreement on the use of specific assessment instruments, this research utilized five privacy questions that addressed the collection and control of information (similar to Maholta), for gaining an understanding of how privacy influences technology use for the case study organization. This approach was selected to minimize the size of the survey, yet still be able to provide insight into different aspects of privacy for analysis (customer and representative views). Since the intention of the case study was not to develop new theories relating to privacy, this approach satisfied sponsor needs and the requirements of the research.

### **RESEARCH METHODOLOGY**

This case study was based on survey data obtained from a global direct sales organization during a four week period in June and July of 2014. An established research strategy, surveys were used for data collection [1]. The survey was cross sectional; where the data was collected at one point in time and was administered through Checkbox, an internet survey tool. One of the objectives for the study was to address a number of questions relating to concerns about internet security in the organization and how these concerns may be related to the use of technology by direct sales representatives. Specific research questions addressed included:

- R1. How frequently is technology and social media used by direct sales representatives?
- R2. How do concerns over internet privacy relate to intention to use technology and actual use?
- R3. How do concerns about privacy and security relate to attitudes toward the importance of technology to increase sales, service customers, and support learning?
- R4. Do significant differences in privacy concerns exist amongst age groups, role, education levels, income levels or years spent in the business?

#### **Survey Instrument**

The survey instrument was developed in a three step process. In the first step, an interview was conducted with corporate marketing, a direct sales manager and a direct salesperson to gather information about the types of technologies and social media being used in the business and their attitudes about the use of the technology. From the interviews, various business functions such as recruiting, sales, education, marketing, and team communications were identified along with a number of technologies being used both at the corporate level and by individual direct salespersons.

After defining the uses of technology and social media, the second step was to define response categories and scales to gather information about participant attitudes and frequency of use for the various tools, and to understand their concerns about internet privacy. To collect frequency of technology usage information, a six point scale ranging from “not at all” to “several times a day” was developed, while attitude scales were measured using a five point Likert type scale that ranged from strongly disagree to strongly agree. Multiple job roles were defined, but were operationalized into two categories representing management and non-management. Several age groupings were defined and were subsequently re-categorized into “Gen Y”, “Gen X”, and “Boomers” based on the birth year of the participant. Additionally, an open ended question was included in the survey that asked participants to discuss concerns they had about using technology in their business. In order to collect information about internet privacy concerns, a previously validated scale was adapted for terminology use in this survey. The questions relating to internet security privacy are indicated in Table 3 below.

**Table 3.** Internet Privacy Questions

Q1	I am concerned about internet privacy when I use the internet
Q2	I am concerned about people who I do not know obtaining information about me from my online activities

Q3	My customers are concerned about online privacy
Q4	My customers are concerned about providing credit card information online
Q5	I am concerned about people online being who they say they are

### Survey Distribution and Administration

The last step in preparing the instrument was to test it on a Director and sales representative to insure that the terminology used was understandable in the organization. After making some wording changes, the survey was finalized and was distributed by the Director sponsoring the research to approximately 60 other Directors. These Directors were then encouraged to distribute the survey to sales representatives that they worked with to obtain broad geographic responses. Because the number of individuals working with each Director was not known, it is not possible to calculate an overall response rate, however a total of 270 valid responses were received for the survey. To encourage participation, a drawing from a list of all of the respondents was held and an Apple iPad was awarded to one individual after the survey was closed.

Once all responses were received, SPSS was used to analyze the responses. Frequency distributions for the questions were reviewed and Chi-square analysis was performed to determine if relationships existed between internet privacy concerns, and the use of technology and social media. Factor analysis was performed on the questions including those relating to internet privacy to insure that the groups of questions were measuring similar concepts. Additionally, relationships were explored between internet privacy concerns and how technology was being used by the sales representatives. Lastly, content analysis was performed on the open-ended survey responses to gain an understanding of concerns that inhabit the use of technology by the participants.

## RESULTS

### R1. How frequently is technology and social media used by direct sales representatives?

A large percentage of direct sales representatives use personal Facebook accounts (88%) personally and to support their social network of friends. A similarly high percentage of representatives use a personal website (86%) to conduct their business. A smaller percentage (50%) indicated that they used Facebook business fan pages. Although the direct sales company offers a number of web sites and uses a number of social media sites, the representatives generally had limited knowledge of whether their customers were accessing the sites (e.g. 70% did not know if customers accessed the corporate fan page and 84% did not know if they accessed other social media sites offered by the company). Another indicator of technology usage reported was that the average number of friends on Facebook was 329, while the average number of likes on the business page was 42. The Facebook friend reported is similar to averages reported by Pew [14] which would suggest a pattern of usage similar to the general public. Table 3 below summarizes technology and social media use in the case.

**Table 4.** Technology Usage Percentage of Respondents

<b>Technology</b>	<b>Not At All</b>	<b>Infrequent</b>	<b>Frequent</b>
Facebook (personal)	12	40	48
Facebook (business)	50	33	17
YouTube	53	37	10
Instagram	78	18	4
Videoconferencing	73	23	4
Polyvore	96	3	1
LinkedIn	51	46	3
Personal Web Site	14	65	21

**R2. How do concerns over internet privacy relate to intention to use technology and actual use?**

The next step in the process was to evaluate whether any statistically significant relationships existed between concerns over internet privacy and the use of technology (including social media) by the direct salespersons.

An analysis was performed to assess whether relationships existed between participants intention to continue to use technology and social media and their level of privacy concern. A significant relationship was found ( $\chi^2=22.358$ ,  $df=6$ ,  $p=.001$ ). Those most likely to continue to use technology had the least level of privacy concern. A more specific analysis examined whether privacy concerns were related to frequency of usage of a participant’s business Facebook site, and no significant relationships were found.

Additionally, the relationship between level of privacy concerns and the frequency with which participants posted content on the internet was assessed. Based on the survey responses, a significant relationship was identified where those with lower levels of privacy concern had the most frequent postings ( $\chi^2=10.480$ ,  $df=4$ ,  $p=.033$ ).

To gain additional understanding of concerns about privacy and how it impacted participants use of technology and social media, a content analysis of open ended participant responses was performed. The question “what reasons limit your use?” of social media and personal web sites (business) was asked. Approximately 20% (54 out of 270) of the respondents indicated that fraud, security or identity theft concerns limit their use of the technology.

**R3. How do concerns about privacy and security relate to attitudes toward the importance of technology to increase sales, service customers, and support learning?**

This question is intended to provide context for potential explanation of the privacy paradox where participant’s behavior may be different than what would be expected. Table 4 provides a summary of responses relating participant attitudes on the importance of technology to support education and their business, and to improve sales. The functions indicated provide value or benefits to the organization or individual. Between 72% and 81% of the respondents agreed that technology was important for support, while a smaller 37% to 58% agreed on the importance of technology to help to grow the business.

**Table 5.** Importance of Technology for Business Functions

Function	Disagree %	Neutral %	Agree %
Recruiting	19	44	37
Increase sales	6	38	56
Acquire new business	10	32	58
Service customers	6	19	75
Market my business	3	22	75
Maintain relationships	2	18	80
Communications	2	16	81

The next step in the process was to perform t-tests to assess if differences existed between attitudes toward the importance of technology enabled business functions and whether participants were “concerned about privacy” or “not concerned about privacy”. The survey responses for strongly disagree, disagree, and neutral were re-categorized as “not concerned”, while responses for agree and strongly agree were re-categorized as “concerned” about privacy for analysis purposes. The null hypothesis for each of the tests was that there were no differences in mean responses between concerned/not concerned participants and the importance of technology enabled business functions. The findings suggest that there were no significant differences between the means in attitudes about the importance of the technology enabled business functions and where privacy concerns were present. Of the 270 responses, 82 were categorized as “not concerned” while 188 were categorized as “concerned”. This finding suggests that although privacy concerns exist, technology is still believed to be important for the operation and support of various business functions by both concerned and not concerned individuals.

**R4. Do significant differences in privacy concerns exist amongst age groups, role, education levels, income levels or years spent in the business?**

The last area of investigation was to determine if relationships existed between privacy concerns and a number of variables of interest. A statistically significant relationship was found to exist between level of privacy concern and age groups. However, for the other major variables assessed (role in organization, years selling the product, education level, and income level), no statistically relevant relationships were found with level of privacy concern.

With respect to age and privacy concerns, GenY participants had the least concerns regarding privacy while the boomers had the most concerns about privacy. Gen X indicated higher concerns than the Gen Y respondents and fewer concerns than the boomers. A statistically significant relationship existed between level of privacy concern and age ( $\chi^2=12.780$ ,  $df=4$ ,  $p=.012$ ).

### **CONCLUSIONS**

Although a relatively high percentage of participants (69%) indicated a continued intention to use technology and social media, a similarly high percentage (69%) indicated concerns about internet privacy. In addition, based on open ended survey question responses, 54 out of 270, or 20%, indicated that privacy concerns limit their use of technology. These findings are consistent with prior research that suggests that a privacy paradox exists [17] where users continue to use internet technology even though they have concerns about privacy in that environment. In the case company organization, further analysis suggested a possible reason why the paradox might exist. One potential reason is that both those with concerns about privacy and those with no concerns had no statistical differences in their attitudes about the importance of technology to support their businesses. In this instance, the value of technology to support business functions may have provided sufficient motivation for users to use the internet technology in spite of concerns about privacy.

Based on prior research, the existence of relationships between age, posting frequency, and the intention to use technology were expected and supported by the analysis.

### **Implications for the Business**

Despite a significant number of participants using technology and social media in their business, concerns about internet privacy have limited the adoption and utilization of technology to support various business functions. Given the pervasive use of technology in society, individuals and organizations that do not take advantage of technology risk loss of business, limit their ability to grow, and have the potential for poor customer service and support.

Approaches that can be considered by the organization to help improve technology adoption and to minimize risk include the following:

- Identify and disseminate best practices regarding securing information and protecting customer data
- Conduct education sessions with direct salespersons on how current technology protects electronic content
- Provide automated updates and enhancements to software products made available to salespersons to insure minimization of vulnerabilities
- Provides guidelines and practices on the use of social media including recommended security settings
- Provide education on PCI (credit card processing) requirements (legal and technical)

Other actions that can be taken by the direct salespersons and the direct selling company include conducting benchmarks with other direct sales organizations, gather and assess field experiences relating to security breaches, and monitor on-going training efforts relating to security to enhance compliance.

### **Limitations**

Since this was a case study for a single organization, it is not possible to generalize the results to other organizations. In addition, since there were some limitations relating to the scope of the survey instrument, not all possible dimensions of available security scales could be implemented. These limitations suggest opportunities for expanding

the scope of the research to include other direct sales organizations to determine if consistent patterns of usage and levels of concern exist. More importantly, further analysis may help to define a framework for potentially reducing privacy concerns, improving awareness of risk mitigation strategies, and increasing utilization of technology to support and grow business operations. In addition to survey research, a mixed methods approach with focus groups should be considered to gain a better understanding of the barriers that reduce the use of technology and to begin the process of developing more advanced processes for securing information.

## REFERENCES

1. Babbie, E. (2011). *The practice of social research*. Belmont, CA: Thomson.
2. Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 35(4), 1017-A36.
3. Buchanan, T., Paine, C., Joinson, A., & Reips, U. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165.
4. Claybaugh, C. C., & Haseman, W. D. (2013). Understanding professional connections in LinkedIn - A question of trust. *The Journal of Computer Information Systems*, 54(1), 94-105.
5. Dillon, T. W., & Lending, D. (2010). Will they adopt? Effects of privacy and accuracy. *The Journal of Computer Information Systems*, 50(4), 20-29.
6. Direct Selling Association. What is direct selling? Direct selling 411. Retrieved from <http://www.directselling411.com/about-direct-selling>
7. Direct Selling Association. (2015). Retrieved from <http://www.dsa.org/about-dsa/faqs>
8. Ferrell, L., & Ferrell, O. C. (2012). Redirecting direct selling: High touch embraces high-tech. *Business Horizons*, 55, 273.
9. Glenn, B. (2011). The social media phenomenon. *Direct Selling News*, 7(9), 11-18.
10. Hong, W., & Thong, J. Y., L. (2013). Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly*, 37(1), 275-298.
11. Information Shield. (2015). United States privacy laws. Retrieved from <http://www.informationshield.com/usprivacylaws.html>
12. Leonard, L. N. K. (2012). Attitude influencers in c2c e-commerce: Buying and selling. *The Journal of Computer Information Systems*, 52(3), 11-17.
13. Malhorta, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC); the construct, the scale, and a causal model. *Information Systems Research*, 15(4), 336-355.
14. Pew Research Center. (2015). 6 new facts about Facebook . Retrieved from <http://www.pewresearch.org/fact-tank/2014/02/03/6-new-facts-about-facebook>
15. Ponder, K. (2011). The ultimate social business model. *Direct Selling News (Supplement to the Wall Street Journal)*, , 05-01-2015.
16. Ponemon. (2014). 2014 cost of cyber crime study. Retrieved from <http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report>
17. Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human Computer Studies*, 71, 1133.
18. Privacy Rights Clearinghouse. (2013). Chronology of data breaches. Retrieved from <https://www.privacyrights.org/data-breach>
19. Roush, C. (2015). The pulse of today's party. Retrieved from [http://directsellingnews.com/index.php/view/the\\_pulse\\_of\\_todays\\_party#.VWDFFljbLrc](http://directsellingnews.com/index.php/view/the_pulse_of_todays_party#.VWDFFljbLrc)
20. Sim, I., Liginlal, D., & Khansa, L. (2012). Information privacy situation awareness: Construct and validation. *The Journal of Computer Information Systems*, 53(1), 57-64.
21. Small Business Association. (2012). Retrieved from [https://www.sba.gov/sites/default/files/FAQ\\_Sept\\_2012.pdf](https://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf)
22. Smith, J. H., Milberg, S. J., & Burke, S. J. (1996). Information privacy; measuring individuals concerns about organizational practices. *MIS Quarterly*, 20, 167-196.
23. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, 35(4), 980-A27.
24. Warren, S., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4, 193-220.

25. Westin, A. (1967). *Privacy and freedom*. New York: Atheneum:
26. Worldwide Direct Selling Association. (2015). What is direct selling? Retrieved from [http://www.wfdsa.org/about\\_dir\\_sell/index.cfm?fa=whatids](http://www.wfdsa.org/about_dir_sell/index.cfm?fa=whatids)