Chapter 74
Why We Disclose Personal Information Despite Cybersecurity Risks and Vulnerabilities:
Obligatory Passage Point Perspective

Patrick I. Offor
City University of Seattle, USA

ABSTRACT

Is it fair to say that the disclosure of personal information, in an online setting, is voluntary or due to incentivization, cognitive risk-benefit analysis, cognitive predisposition, or based on information sensitivity, whereas our personal information is being collected, knowingly and forcibly most of the time, and unknowingly and inadvertently at other times? While the collection of personal information is necessary to organizations and online users alike, in completing online transactions, the issue is the collection of additional non-pertinent information that serves only organizations' prescriptive and predictive analytics and their business interests, and not the users'. Most study on the phenomenon have centered on voluntary or willful disclosure, and on technical collections. This article examines the phenomenon based on the concept of the obligatory passage point and found that online users disclose their personal information online mostly because the information are designated as required in an online setting, contrary to conventional beliefs.

INTRODUCTION

Personal information or personal data is the heartbeat or the basis for online transaction processing. In other words, the disclosure of personal information is the bedrock upon which electronic activities, over the Internet, flourishes. Personal information includes personal identifiable information, personal financial information, and personal healthcare information. Some personal information can be classified

DOI: 10.4018/978-1-5225-8176-5.ch074

as sensitive or confidential. The personal information and online transaction relationship is such that an online user would always be required to provide some sort of personal data in any human-internet interaction for proper identification, authentication, payment, and for ensuring the completeness of the transaction, whether the transaction is for goods or for services. Completeness of a transaction involves all activities from the initiation of a transaction to the receipt of the goods or services.

The numbers of online transactions are on the rise because the number of users of internet capable devices and the number of organizations with online presence have increased dramatically in the U.S., and around the world (Offor, 2016). Therefore, the need for organizations to obtain, store, and use or deploy their online users' personal information in electronic commerce or business (e-commerce or e-business), electronic government (e-government), electronic healthcare (e-healthcare), electronic marketplace (e-marketplace), online banking, and the like has grown exponentially.

Sadly, the same personal information has also become the main target of cybersecurity incidents and attacks, from malicious and non-malicious attackers, because of the central role it plays in advancing online transactions. The largest exposures of data breaches, around the world, have occurred in the last couple of years. Among them are (1) the 3.0 million records exposed at Yahoo in 2016, (2) the 2.0 billion records at DU Caller Group, in China, in 2017, (3) the 1.3 billion records at River City Media, in the U.S., in 2017, (4) the 1.2 billion records at NetEase Incorporated (dba 163.com), in China, in 2017, (5) the 1.1 billion records at Aadhaar database, in India, in 2018, and (6) the 711 million records from a misconfigure spambot database, in the Netherlands, in 2017 (Risk Based Security Report, 2018). Furthermore, the average cost of each lost or stolen record that has sensitive or confidential information was $141 in 2016 and the average total cost of data breach was $3.62 million in the same year, according to the 2017 Cost of Data Breach study, which involved 419 companies in 13 countries (Ponemon Institute Report, 2017). Henceforth, while the costs associated with cybersecurity attacks and the possibility of loss of revenue from negative media coverage inform organizations' cybersecurity concerns, the lack of control of personal information informs online users' concerns. Meanwhile, the costs of data breaches increased by 6.4% in the 2017 and the cost of each stolen record rose to $148 (Ponemon Institute Report, 2018).

The issue, today, is that users have limited to no control of their personal information. This lack of control on the collection, use, and storage of personal information has exacerbated users' information privacy concerns. Additionally, recent news of reporting delays, reactionary nature of cybersecurity incidents and attacks, and a shift in website analytics demand, from metrics to descriptive, from descriptive to predictive, from predictive to prescriptive, and now from prescriptive to causation—combination of descriptive and prescriptive analytics (Bekavac & Pranicevic, 2015; Fitz-enz, 2009), have not helped in reducing users' concerns. In a privacy and security study, which involved 41,000 households by the U.S. Census Bureau in 2015, Goldberg (2016) indicated that American are ambivalent and concerned about data breaches, cybersecurity incidents, and the privacy of online services. The paper suggested, "Forty-five percent of online households reported that these concerns stopped them from conducting financial transactions, buying goods or services, posting on social networks, or expressing opinions on controversial or political issues via the Internet, and 30 percent refrained from at least two of these activities" (Goldberg, 2016).

Surprisingly, but understandably, users have continued to disclose their personal information online despite the constancy of cybersecurity threats and vulnerabilities. Therefore, the motivation for this study is to understand why online users disclose their personal information based on obligatory passage point (OPP). This is necessary because while online users' willful disclosure of personal information and organizations use of technology to collect personal information are well documented in the extant