Concern But No Action: Consumers' Reactions to the Equifax Data Breach

Yixin Zou
School of Information
University of Michigan
Ann Arbor, MI, USA
yixinz@umich.edu

Florian Schaub
School of Information
University of Michigan
Ann Arbor, MI, USA
fschaub@umich.edu

CHI'18 Extended Abstracts, April 21–26, 2018, Montréal, QC, Canada.
ACM ISBN 978-1-4503-5621-3/18/04.
http://dx.doi.org/10.1145/3170427.3188510

Abstract
Following the 2017 Equifax data breach, we conducted four preliminary interviews to investigate how consumers view credit bureaus and the information flows around these agencies, what they perceive as risks of the Equifax breach, and how they reacted in practice. We found that although participants could properly articulate the purpose of credit bureaus, their understanding of credit bureaus' data collection practices was divided and incomplete. Although most of them conceptualized identity theft as the primary risk of data breaches disclosing credit information, and noted a lack of trust/self-efficacy in controlling their data collected by credit bureaus, they did not take sufficient protective actions to deal with the perceived risks. Our findings provide implications for the design of future security-enhancing tools regarding credit data, education and public policy, with the aim to empower consumers to better manage their sensitive data and protect themselves from future data breaches.

Author Keywords
Credit bureaus; data breach; mental model; risk perception; protective behavior; privacy paradox; user-centered design.

ACM Classification Keywords
K.6.5 [Security and Protection]: Unauthorized access

Introduction

Credit bureaus are private, for-profit organizations that create aggregated reports of individual credit information, and offer this information as a service to businesses that need to assess the creditworthiness of their customers in order to make decisions, such as approving loans and issuing new credit cards. In the United States, the Fair Credit Reporting Act (FCRA) regulates activities of credit bureaus. Yet, its effectiveness in protecting consumers is questionable, given that credit bureaus have kept violating the rules and consumers have large amounts of errors on their credit files [10]. Equifax, as one of the big three consumer-focused U.S. credit bureaus (the other two are TransUnion and Experian), experienced a large-scale data breach in 2017, compromising the personal information of over 145 million consumers. While this data breach and related mitigation strategies for consumer have been widely covered by the media, little is known about how consumers perceived the risks stemming from this data breach and how they reacted to it. We present initial findings from an on-going study of these questions, providing additional insights regarding the known gap between security and privacy concerns and behaviors [7], with implications on design, education, and public policy.

Related Work

First, we give an overview of related studies on mental models related to privacy and security, and discuss related work on risk perception and privacy paradox.

Mental Models in Security and Privacy Research

Mental models are the representations of how objects or processes function in people's minds. In privacy and security research, the analysis of mental models has shed light on the gap between their understanding and behaviors, such as why home computer users don't take protective actions against botnets [12] and why people ignore or misinterpret security warnings [2]. Among these mental models, there are also substantial discrepancies between experts and non-experts [6]. For general consumers who are not necessarily financially literate [9] compared to financial experts, little is known about their mental models of credit bureaus and risks associated with credit information. Studying mental models in this context, therefore, may provide insights on consumers' reasoning, decision-making and behavior related to the Equifax data breach in particular, and credit bureaus and data breaches in general.

Risk Perception

Mental models have been used to study risk perception — people's subjective assessment of the probability that a specific event happens and how concerned they feel about its consequences. There are various determinants of risk perception [11], including people's dread and novelty to the event, attitudes and beliefs, general sensitivity to risks, and many others. Previous work showed that consumers have a significant increase of fear about being identity theft victims after data breaches [5], yet it remains unknown what contributes to such increase, and whether this changes their sentiment to the company or results in protective behavior. This study aims to fill this gap by exploring whether identity theft, being defined as the primary risk of the Equifax breach by authorities [4], is conceptualized in a similar way by consumers, and moreover, the factors, if any, that lead to the perceptual difference of risks among individuals.

Privacy and Security Concerns and Behaviors

Hackers' unauthorized access to consumer data at Equifax can be considered an invasion of personal privacy. Privacy concerns about the Equifax data breach have been noted in news [1], and we intend to provide an academic investigation for this. Furthermore, evidence has shown that con-

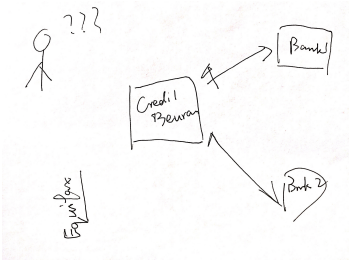

Figure 1: Example of mental model with limited sources identified.

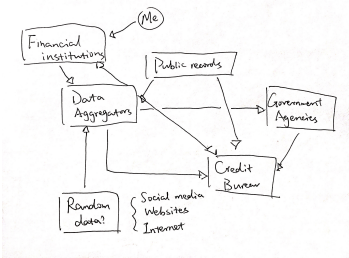

Figure 2: Example of mental model with comprehensive sources identified.

sumers might not translate their concerns into actions, as demonstrated by a less than 1% increase of credit freezes at TransUnion shortly after the breach [13]. This implies the possibility of a pattern similar to the "privacy paradox" [8]: people may claim they care about the security of their credit data, while in reality they compromise it for small benefits or conveniences (e.g., time and money saved for not initiating a credit freeze). While scholars have examined the privacy paradox primarily in the context of social networking sites and transactional situations [8], we extend this line of research by investigating this phenomenon in the context of data breaches.

Methodology

Following previous studies on mental models [12, 14], we conducted semi-structured interviews to investigate how participants think credit bureaus operate in general, and their risk perceptions and actions regarding the Equifax data breach. We first asked participants about ways they manage their personal finances, leading into a discussion about experiences with credit bureaus. We arranged a drawing activity to elicit their mental models. Next, we provided a basic background of the Equifax breach for those who hadn't heard of it. We probed risk perception by asking them what they thought as consequences of the breach and what they could do about it. Finally we went through a list of protective strategies with questions about the experiences and expected outcomes related to each. The study was determined to be exempt by our institution's IRB.

Here, we report preliminary results from initial interviews with four participants recruited using convenience sampling in the U.S. Midwest in October 2017. We framed the study focus as personal finance and credit bureaus to avoid priming participants with Equifax or any security awareness. All participants were males in their 20's and 30's, primarily working at a university, with various educational and income levels. Three of them were U.S. citizens or permanent residents. All interviews were audio-recorded and transcribed before analysis. We followed an inductive, open coding process for the data analysis.

Preliminary Findings

We discuss our preliminary findings grouped according to our research questions: mental models, risk perception, and protective actions.

Incomplete Understanding of Data Collection Practices
All participants could correctly interpreted credit bureaus' purpose as assigning credit scores to individual consumers. A few went forward to describe the purpose on a conceptual level (e.g. *"decide [how much] you are worth lending money to" (P2)*) and discussed how these scores helped businesses make decisions.

In contrast, participants demonstrated a varied understanding of the information providers of credit bureaus, albeit they all stated that the information collected was "a large amount". For instance, P1 only identified banks (see Figure 1), whereas P2 developed a more holistic view that also included implicit information exchange processes between different parties (see Figure 2). Two participants (P2 and P4) who had read their credit reports offered much more details about types of information collected, covering personal to financial data, while others who had not looked at their credit reports seemed to be guessing (e.g. *"breach of contracts was the only thing"* (P3)).

Participants' understanding of who has access to collected data by credit bureaus also varied. All participants were able to identify financial institutions, whereas other public (e.g., government agencies) or private parties (e.g., car dealerships) were mentioned much less often. In particular,

P1 noted that he checked his credit score at Chase, but was quite confused about what the score represented and how it was generated.

Risk Perception, Trust, and Self-efficacy in Control
Three out of four participants showed a certain extent of awareness about the 2017 Equifax data breach: P3 had a rough idea that *"something got hacked"*; P2 and P4 gave more details about how the breach was caused, and what types of information were exposed. All participants mentioned identity theft as the potential consequence of this breach, mostly in an implicit way (e.g., *"What they would be able to do is kind of stealing my report, applying additional credit card or something, so that's how I might be affected."* (P1)). Yet the awareness of identity theft risk didn't always come with the concern of being personally affected. For instance, P3 stated he didn't think he would be affected much as he had no credit card.

A lack of trust and self-efficacy was noted in the discussion of risk perception. Participants generally held a negative perception of the breach, either *"felt vulnerable"* (P1), or didn't experience a significant attitudinal change because their trust in the whole credit reporting system had been eroded: *"I thought it was garbage anyways. I don't think any of our data is actually pretty secure"* (P2). P4 also extended the lack of trust to other credit bureaus and institutions who held similar sensitive data. Another issue is the perceived lack of self-efficiency in controlling their data. For instance, P2 claimed that *"I don't have any control of the data. I only have control over the monitoring."* P4 followed up with the suggestion that *"There should just be a law that says if this company has information about you, then [they] must offer you protection. You need to be able to have control of the data to some extent."*

Lack of Protective Actions
While concerns of the Equifax breach were prevalent, only P2 and P4, with a more well-rounded knowledge of their credit status and the Equifax data breach, properly articulated potential strategies and took actions to cope with the perceived risks. Both learned they might be affected from the Equifax website. Following that, P4 placed a credit freeze in all three big bureaus, which hinders others from opening new accounts that require credit checks in one's name. P2 mentioned he more frequently monitored account activity through Mint, which is more effective in preventing misuse of current accounts. Neither of them seemed to consider and implement all potential strategies to deal with different types of identity theft.

We identified several factors that might explain the negligence of protective actions. Lack of knowledge about existing measures appears to be a prominent issue. While P1 showed high concerns about his data security at Equifax, when asked how to check if he was affected by the breach, he stated *"I don't know how I would do that."* Another significant factor is cost: among th three participants who were aware of the breach, only P4 paid to initiate his credit freezes. The others either chose a more economic option (P2), or remained inactive to avoid costs (P3). In addition, usability issues not only deterred participants from taking actions, but also affected their experience: P3 said he could not check his breach status on Equifax's site since it asked for his SSN, which he did not have; P4 described the process of placing credit freezes as time-consuming, tedious, and intransparent.

Discussion

In line with previous suggestions that risk communication models should be developed based on non-experts' mental models [3], our study provides the viewpoint of general

consumers regarding the interpretation of functions and information flows of credit bureaus. Although we refrain from drawing final conclusions based on the small sample size and gender-biased sample, our initial findings already indicate important implications for interaction design, security education, and public policy.

Awareness of Risk Does Not Lead to Actions
Our study contributes to existing literature by showing that participants' mental models of credit bureaus and their risk awareness were not the primary factors affecting their protective behavior. All participants were able to recognize identity theft as the primary risk, regardless of their knowledge and understanding of how credit bureaus work. Though participants with more articulated mental models were more aware of available protective actions, their decisions of adherence were more heavily influenced by other factors, such as cost and usability issues.

Interactive Design for Better Usability and Transparency
Our work contributes to the HCI literature on two aspects. First, we demonstrate the need to fix usability issues of current tools for managing credit data: participants avoided using them due to perceived low trustworthiness, had difficulties navigating them, or complained about the hassles during usage. The notion of teaching consumers how to use these tools rings hollow unless these usability issues are addressed.

Second, we suggest the development of new tools that make credit-related information flows more transparent. One possibility is to develop just-in-time notices informing consumers whenever companies request access to their credit data or when new data is added to their credit file. A further step is to introduce an approval process between credit bureaus and consumers when a credit request is made by a third party, so that consumers have the agency to allow or deny those requests. These steps can potentially reduce consumers' uncertainty about risks and concern about data security as they would be better informed.

Policy and Educational Efforts to Accompany Design Solutions
In addition, regulatory efforts should be made to create stronger incentives for credit bureaus to provide usable protective measures to consumers. The FCRA should be amended to guarantee consumers free and more frequent access, not just to credit reports, but also security functions like credit freezes. Credit bureaus should be supervised more stringently in their operation and security to limit the potential of data breaches at the magnitude of the 2017 Equifax breach.

Educational efforts, furthermore, are needed to make consumers aware of their rights and available choices and guide them to take actions. Since we found that participants had difficulty locating resources for learning their credit status as well as reacting to the Equifax data breach, more efforts should be devoted to improve the financial literacy of consumers [9], both through offering standardized educational programs and making resources more widely accessible online.

Future work

We plan to conduct additional interviews with a more demographically diverse sample to enrich our current findings. We further plan to subsequently conduct a survey to validate the prevalence of identified themes and issues. Finally, our preliminary findings already demonstrate avenues for designing enhanced transparency and control solutions to empower consumers to take a more active role in monitoring and managing their credit data and financial health.

Acknowledgements

This material is based upon work partially supported by the National Science Foundation under Grant No. CNS-1330596.

REFERENCES

1. Ben Berliner. 2017. Equifax breach drives legislative push on data privacy. (2017). https://fcw.com/articles/2017/10/23/data-breach-legislation-berliner.aspx.
2. Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2011. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy* 9, 2 (2011), 18–26.
3. L Jean Camp. 2009. Mental models of privacy and security. *IEEE Technology and Society Magazine* 28, 3 (2009).
4. Federal Trade Commission. 2017. The Equifax Data Breach. (2017). https://www.ftc.gov/equifax-data-breach.
5. Ponemon Institute. 2014. *The Aftermath of a Data Breach: Consumer Sentiment*. Technical Report. https://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.
6. Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices.. In *SOUPS*, Vol. 15. 1–20.
7. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. My data just goes everywhere: user mental models of the internet and implications for privacy and security. In *Proc. of the 11th Symposium On Usable Privacy and Security (SOUPS)*. 39–52.
8. Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (2017), 122–134.
9. Annamaria Lusardi and Olivia S Mitchelli. 2007. Financial literacy and retirement preparedness: Evidence and implications for financial education. *Business economics* 42, 1 (2007), 35–44.
10. Maureen Mahoney. 2014. *Errors and Gotchas: How Credit Report Errors and Unreliable Credit Scores Hurt Consumers*. Technical Report. http://consumersunion.org/wp-content/uploads/2014/04/Errors-and-Gotchas-report.pdf.
11. Lennart Sjöberg. 2000. Factors in risk perception. *Risk analysis* 20, 1 (2000), 1–12.
12. Rick Wash. 2010. Folk models of home computer security. In *Proc. of the 6th Symposium on Usable Privacy and Security*. ACM, 11.
13. Suzanne Woolley. 2017. Few Americans Are Freezing Their Credit After the Equifax Hack. (2017). https://www.bloomberg.com/news/articles/2017-10-06/few-americans-are-freezing-their-credit-after-the-equifax-hack.
14. Yaxing Yao, Davide Lo Re, and Yang Wang. 2017. Folk Models of Online Behavioral Advertising. In *Proc. of the 2017 ACM Conf. on Computer Supported Cooperative Work and Social Computing (CSCW)*. 1957–1969.