The "Identity Literacy" Scale: A Preliminary Report

Matthew S. McGlone
Dawna I. Ballard
Brenda Berkelaar
Maxim Baryshevtsev
Laura Brown

2015
UT CID Report #1502

This UT CID research was supported in part by the following organizations:

identity.utexas.edu
Identity theft has become the defining crime of the information age, with an estimated 13 million or more incidents each year in the U.S. alone (Finklea, 2014). Publicity generated by news coverage of severe cases of identity theft as well as various information campaigns in the public and private sector have raised consumer awareness about pernicious crime (Greis, Nogueira, & Kellogg, 2012). Arguably, however, relatively few consumers are aware of different identity theft varieties, which can range from minor swindles to major heists and are perpetrated by a broad spectrum of offenders, from family members to shadowy, international gangs.

The rapid proliferation of educational materials about identity theft (e.g., Madden, Lenhart, Cortesi, & Gasser, 2013) warrants the development of an instrument for measuring consumers’ “baseline” understanding of the issue and the impact these materials may have on their subsequent beliefs, attitudes, and behaviors. We report here the preliminary results of our efforts to create and validate such an instrument.

Scale Design
The assessment instrument consisted of four sections designed to measure awareness of different aspects of identity theft as suggested by Finklea (2014). Each section began with an open-ended query: Respondents were presented with a definition of the aspect and asked to generate instances of it from their personal knowledge; subsequently, they reviewed and rated a list of aspect instances we compiled based on recommendations from cybersecurity experts.

The first section measured respondents’ awareness of self-relevant data that meet the definition of “personally identifiable information” (PII) as described by the U.S. Government Accountability Office (2006): “Any information about an individual maintained by an organization, including any information that can be used to distinguish or trace an individual’s identity, and any other information that is linked or linkable to an individual.” After attempting to generate instances of PII from their personal knowledge, respondents reviewed instances provided (date of birth, home zip code, social security number, etc.) and rated the perceived “sensitivity” of each instance, defined as “the extent to which you perceive the potential risk of harm to yourself if the information were to fall into the wrong hands and be used without your permission.” These ratings were made on a 7-point Likert-type scale (1 = “not at all sensitive” to 7 = “highly sensitive”).

Subsequent sections employed this format to gauge respondents’ awareness of identity theft harm (i.e., potential negative consequences of having their PII used without their permission, rated on a 7-point likelihood scale); theft prevention (strategies for preventing unauthorized access to their PII, rated on a 7-point effectiveness scale); and post-theft restoration (strategies for repairing the damage caused by unauthorized PII access, rated on a 7-point effectiveness scale).

Sample Recruitment and Survey Procedure
Four hundred (420) respondents were recruited through a post on Mechanical Turk (www.mturk.com), an online platform operated by Amazon.com. MTurk is a crowdsourcing labor market in which employers (“requesters”) post advertisements for human intelligence tasks (“HITs”) and employees (“workers”) perform those tasks for compensation. Participants were paid $1.00 for completing the scale. MTurk workers had to meet two criteria to participate. First, they had to be registered with Amazon.com as residents of the United States. Second, workers were required to have completed at least 100 previous HITs in MTurk and have 95% or higher approval ratings from prior requesters. This requirement was suggested by Eyal, Vosgerau, and Acquisti (2014), who found that “high reputation” workers meeting these criteria are highly likely to follow task instructions and expend adequate effort to generate considered responses.

The scale was administered to respondents as online survey conducted using Qualtrics software (version 18.856s). Respondents gained access to the survey in Qualtrics via an advertisement posted in MTurk recruiting volunteers for a “study of beliefs and attitudes about identity theft.” After providing informed consent and reading a brief overview of the study, participants completed the scale sections in the aforementioned order (PII, Harm, Prevention, and
Restoration). After completion, they read a short debriefing statement and then were provided with a passcode to claim payment in MTurk. On average, participants completed the survey in 16 minutes ($M = 15.36$, $SD = 2.31$).

**Results**

Of the 420 respondents who completed the survey, 21 were deemed to have finished too soon (10 minutes or less) to have taken it seriously and 6 so late (30 minutes or more) as to indicate distraction. Their data were not analyzed further. Demographic characteristics of the retained 393 respondents are reported in Table 1.

**Table 1**

*Sample Characteristics (N = 393)*

<table>
<thead>
<tr>
<th>Measure</th>
<th>n</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>206</td>
<td>47.3</td>
</tr>
<tr>
<td>Female</td>
<td>186</td>
<td>52.4</td>
</tr>
<tr>
<td>Transgender</td>
<td>1</td>
<td>0.3</td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18-29</td>
<td>159</td>
<td>40.5</td>
</tr>
<tr>
<td>30-39</td>
<td>114</td>
<td>29.0</td>
</tr>
<tr>
<td>40-49</td>
<td>54</td>
<td>13.7</td>
</tr>
<tr>
<td>50-59</td>
<td>35</td>
<td>8.9</td>
</tr>
<tr>
<td>60 and Older</td>
<td>31</td>
<td>7.8</td>
</tr>
<tr>
<td>Race</td>
<td></td>
<td></td>
</tr>
<tr>
<td>White</td>
<td>313</td>
<td>79.6</td>
</tr>
<tr>
<td>Hispanic/Latino</td>
<td>23</td>
<td>5.9</td>
</tr>
<tr>
<td>Black</td>
<td>25</td>
<td>6.4</td>
</tr>
<tr>
<td>Native American/Alaskan</td>
<td>6</td>
<td>1.5</td>
</tr>
<tr>
<td>Asian</td>
<td>24</td>
<td>6.1</td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
<td>0.5</td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Did Not Complete High School</td>
<td>2</td>
<td>0.5</td>
</tr>
<tr>
<td>High School Graduate or GED</td>
<td>49</td>
<td>12.5</td>
</tr>
<tr>
<td>Some College</td>
<td>105</td>
<td>26.7</td>
</tr>
<tr>
<td>Two-Year College Degree</td>
<td>52</td>
<td>13.2</td>
</tr>
<tr>
<td>Four-Year College Degree</td>
<td>150</td>
<td>38.2</td>
</tr>
<tr>
<td>Master’s Degree</td>
<td>28</td>
<td>7.2</td>
</tr>
<tr>
<td>Doctorate</td>
<td>2</td>
<td>0.5</td>
</tr>
<tr>
<td>Professional Degree</td>
<td>5</td>
<td>1.3</td>
</tr>
</tbody>
</table>

**Factor Analysis and Scale Reliabilities**

Responses in each scale section were subjected to a principal component factor analysis with varimax rotation in order to obtain discrete factors with minimal overlap. The items comprising each factor were averaged into an index for subsequent analysis. The emergent factors in each scale section are reported below (also see Table 2).

**PII Awareness Factors.** Respondents sensitivity ratings of what constitutes PII clustered into 5 distinct factors: “Stable Individual Characteristics” (9 items, explaining 23% of rating variance), “Contact Information” (5 items, 12.2%), “Credentials” (5 items, 11.5%), “Behavioral Data” (5 items, 11.3%), and “Common Authentifiers” (2 items, 6.1%). Scale reliabilities ranged from $\alpha = .93$ to .75.

**Harm Awareness Factors.** Two factors emerged from the Likelihood ratings of the potential identity theft: “Identity Threats” (5 items, %) and “Financial Threats” (2 items, %). Scale reliabilities were $\alpha = .90$ and .71, respectively.

**Prevention Awareness Factors.** Three factors emerged from effectiveness ratings of the prevention strategies: “Data Elimination Strategies” (6 items, %), “Disclosure Avoidance Strategies” (6 items, %), and “Data Protection Strategies” (6 items, %). Scale reliabilities ranged from $\alpha = .92$ to .68.
**Restoration Awareness Factors.** Two factors emerged from effectiveness ratings of the restoration strategies: “Immediate Strategies” (8 items, %) and “Long-Term Strategies” (3 items, %). Scale reliabilities were $\alpha = .94$ and $.77$, respectively.

**Table 2**

**Factors in Each Scale Section**

**PI Awareness**

**“Stable Characteristics”** (9 items)
- First Name
- Middle Name
- Sex
- Race/Ethnicity
- Height

**“Contact Information”** (5 items)
- Last Name
- Home Address
- Zip Code

**“Credentials”** (5 items)
- Social Security #
- Driver’s License #
- Credit Card #

**“Behavioral Data”** (5 items)
- Credit Rating
- Salary
- Online Search History

**“Common Authentifiers”** (2 items)
- Mother’s Maiden Name
- Date of Birth

**Harm Awareness**

**“Identity Threats”** (5 items)
- Open Bank Accounts
- Apply for Loans
- Apply for Medical Benefits

**“Financial Threats”** (2 items)
- Make Unauthorized Purchases
- Sell PII to a Third Party

**Prevention Awareness**

**“Data Elimination Strategies”** (6 items)
- Shred Receipts
- Erase Hard Drives

**Carefully Read Privacy Policies**
**Update Software Versions**
**Opt Out of Share PII Agreements**
**Install Anti-Virus Software**

**“Disclosure Avoidance Strategies”** (6 items)
- Personally Place Paper Mail in Mailbox
- Have Checks Sent Home
- Don’t Use Simple Passwords
- Don’t Use Public WiFi Networks
- Share SSN Only with Close Family/Friends
- Don’t Carry Medical Insurance ID on Person

**“Data Protection Strategies”** (6 items)
- Financial Documents in Lockbox
- Share Health Info with Caution
- Do Not Click on E-mail Links
- Remove Paper Mail from Mailbox
- Provide PII Only Through Encrypted Sites
- Regularly Order Credit Reports

**Restoration Awareness**

**“Immediate Strategies”** (8 items)
- Create ID Theft Report
- Order Credit Reports
- Create Initial Fraud Alert
- Dispute Errors in Credit Report
- Collect Info About Accounts Compromised
- Contact Fraud Departments
- Ask Companies to Block Transactions
- Submit Report to FTC

**“Long-Term Strategies”** (3 items)
- Renew Fraud Alert After 90 Days
- Check Credit Reports Every 4 Months
- Stop Companies from Debt Collection

**Demographic Comparisons**

**Gender.** Female respondents perceived two categories of PII to be more “sensitive” (to create personal harm if compromised) than males: “Stable characteristics” and “Behavioral Data” ($p <.01$ in both cases). Females also viewed Data Elimination and Data Protection strategies for preventing identity theft to be more effective than did males ($p <.001$ in both cases).
Age. Respondents 40 and over perceived all of the PII categories to be more sensitive than their younger counterparts (p <.001), with the exception of “Stable Characteristics.” They also considered Long-Term strategies of restoration to be more effective than younger respondents, p <.01.

Education. Educational attainment was generally associated with higher perceived PII and prevention awareness. Respondents with 4-year or more advanced degrees viewed all PII categories as more sensitive than others with less education, p <.001 in all cases. They also perceived Data Elimination and Protection prevention strategies as more effective (p <.001), but not Disclosure Avoidance strategies. Finally, they considered both Immediate and Long-Term Strategies of restoration more effective than others at lower educational levels, p <.01.

Income. Respondents reporting annual incomes of $75,000 or more perceived the PII categories “Credentials” and “Behavioral Data” to be more sensitive than lower incomes, p <.001. They also perceived Data Elimination and Protection prevention strategies as more effective than lower earners, p <.001.

Identity Theft Experience. Former victims of identity theft viewed all PII categories as more sensitive than non-victims with the exception of “Stable Characteristics,” p <.01 in all cases. They also considered “Data Elimination” prevention strategies and both categories of restoration categories to be less effective than non-victims, p <.001 in both cases.

Conclusions and Future Directions
The recent push in the public and private sectors to promote identity theft awareness among consumers is laudable. However, there is a dearth of research on the best strategies for teaching “financial literacy” in general and no research on educating people about the determinants and consequences of identity theft and fraud in particular. An important first step in this research agenda is creating a psychometrically sound measure of people’s awareness of identity theft aspects (what counts as PII, the consequences of having it stolen, and strategies for preventing theft and repairing its damages). The goal of the reported study was to create and validate such a measure. The developed measure is suitable for measuring consumers’ baseline understanding of identity theft as well as the impact that educational efforts may have on their understanding.

The next step in our agenda is explore the “calibration” of consumers’ identity theft awareness – that is, the degree to which their perceptions of identity theft correspond with or deviate from those of expert opinion. To this end, our research team will be administering the scale to a panel of cybersecurity professionals. Consensus ratings of this panel will then be used to gauge the accuracy of consumer respondents and to identify where we can improve identity theft awareness and identity literacy via educational efforts.

Identity theft awareness and “identity literacy” are gaining in both importance and attention. Recent well-publicized corporate data breaches as well as the proliferation of more targeted credential thefts are increasing the public’s sense of vulnerability to cybercrime (Finklea, 2014). Consumers may vary widely in their knowledge of identity theft’s causes and awareness of how to protect themselves or recover from it. The scale reported here can be used to measure differences in knowledge and awareness across demographic characteristics and thereby determine which groups will most benefit from identity theft education and what aspects of their knowledge need improvement. Moreover, education and information campaign program evaluators can use the scale to assess the impact of their efforts on consumers’ beliefs, attitudes, and behavior. The introduction of a psychometrically sound “identity literacy” scale is a preliminary but crucial step in moving consumer education about identity theft to a more rigorous, evidence-based practice.

References
© 2015 Proprietary, The University of Texas at Austin, All Rights Reserved.

For more information on Center for Identity research, resources and information, visit identity.utexas.edu.