# “I have nothing to hide; thus nothing to fear”: Defining a Framework for Examining the ‘Nothing to Hide’ Persona

Janine L. Spears and Sheena L. Erete
DePaul University
243 S. Wabash Avenue
Chicago, IL 60604
jspears@cdm.depaul.edu | serete@cdm.depaul.edu

## ABSTRACT

“I’ve got nothing to hide” is a common response when people are asked their view on government surveillance and online tracking for the sake of national security and interest-based advertising, respectively. The ‘nothing to hide’ (NtH) privacy view, characterized by Solove, raises new and important research questions scarcely explored. By clearly conceptualizing the NtH persona, the focus shifts away from whether the person ‘is’ concerned about privacy, to focusing more on ‘why’ concern may (or may not) be needed and how privacy and security scholars and practitioners can better understand and design for this consumer. In this paper, we present a framework to help conceptualize and identify the NtH consumer. We then describe a method to translate the findings from this framework into actionable information that informs design using privacy personas, which are archetypal characters who share common goals, attitudes, and behaviors around privacy. A NtH persona can help to communicate the NtH perspective, prompt new research questions, and positively influence technology design.

## 1. INTRODUCTION

“I’ve got nothing to hide” is a common response when people are asked their view on government surveillance for the sake of national security [17]. In general, the ‘nothing to hide’ attitude toward government surveillance is based on the premise that if one has done nothing illegal or shameful, then the likelihood that one will be harmed from the government’s information collection on one’s comings and goings is minimal. The ‘nothing to hide’ (NtH) perspective may also be applied to the context of online behavioral tracking (‘online tracking’). Similar to government contexts, the NtH attitude toward online tracking assumes that data collection (e.g., web sites visited, online searches made) is done by reputable organizations with reasonably honest intention (e.g., to serve customized ads). From a NtH perspective, if a person is not visiting ‘shameful’ or ‘bad’ web sites, then he/she has nothing to hide and thus nothing to fear from data collected during routine communication and online browsing.

Although the NtH privacy view characterized by Solove [17] raises many new and important research questions, there is scarce empirical research on this consumer segment. Much of the literature on consumer privacy has centered on the concept of ‘privacy concern.’

Indeed, a person who subscribes to the NtH perspective could be studied through the lens of privacy concern. The NtH consumer conceivably has no-to-minimal privacy concern. However, rather than study the NtH perspective solely as one having a negligible level of privacy concern, we suggest that the NtH perspective could be more richly studied by conceptualizing this consumer as a distinctive segment.

In more clearly conceptualizing the NtH consumer, the focus shifts away from whether the person ‘is’ concerned about privacy, to focusing more on ‘why’ concern may (or may not) be needed. That is, ‘privacy concern’ implies that consumers are concerned, at least to some degree, about information privacy. ‘Privacy concern’ frames the privacy discussion around how an individual will behave, given their level of concern. More specifically, studying one’s privacy concern leads us to focus on dependent variables such as the willingness to disclose information or complete a transaction.

In contrast, studying ‘nothing to hide’ as a distinct privacy segment assumes a person has a ‘transparency’ view of privacy and is not concerned with information privacy in day-to-day transactions. Consequently, the NtH consumer leads us to ask a different set of (research) questions than are asked for consumers with privacy concern. The NtH perspective makes us question whether consumers should in fact be more prudent, and more importantly, why. The NtH persona prompts us to discuss in greater detail the actual threats one can face by freely sharing (digital) information. That is, the NtH perspective frees us to assume that consumers will indeed disclose information, and instead prompts us to consider the implications of uninhibited disclosure. Thus, an examination of NtH takes on a risk-based discussion from the consumer’s perspective.

Whereas consumer ‘privacy concern’ prompts important questions with a short time horizon (e.g., whether to disclose information in a given transaction), the NtH perspective prompts us to consider the longer-term implications of unbridled, cumulative information disclosure. For example, in arguing why privacy matters, even when one has nothing to hide, Daniel Solove [18] identified at least four threats to privacy (secondary use, aggregation, exclusion, and distortion) that intuitively increase over time as more data is collected on an individual. Studying the NtH perspective forces us to move beyond discussions of ‘disclosure’ to further studying harmful threats [18] that may be realized by

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA.

consumers as information profiles accumulate over time in an era of Big Data and 'interest-based advertising.'[1]

NtH compels us to consider 'why' individuals should be concerned about information privacy. The NtH consumer also prompts us to consider whether, and if so how, to educate individuals about potential longer-term threats related to information disclosure.

This paper defines a framework with three dimensions that characterize consumers with a 'nothing to hide' perspective and provides insight on how to create privacy personas to communicate the NtH perspective. Our framework provides greater conceptualization and identification of this consumer segment, laying a foundation for theorizing in a variety of areas. For example, bringing to life a NtH consumer through the use of a persona may aid in conceptualizing how the NtH consumer generally perceives and treats risk. How do NtH consumers tend to treat customer privacy (or adhere to security policy) at their respective jobs where they are expected to protect their organization's customer data? What factors influence the NtH persona toward or away from greater privacy concern? Secondly, in addition to theorizing, a NtH persona provides a clearer conceptualization for human computer interaction (HCI) design of privacy-enhancing technologies (PET). Given that there is general public consensus that information privacy is needed in certain contexts (e.g., electronic payment transactions), a greater understanding of the NtH persona can aid technology designers develop more effective privacy protections that reach this consumer segment.

In the remainder of this paper, we describe what personas are and their value, followed by a discussion on consumer segmentation and personas in the privacy literature. Next, we define three dimensions that help operationalize the NtH perspective, followed by a discussion on how data from this framework can communicate the NtH perspective using privacy personas. We then provide an illustration using a fictitious NtH persona. Finally, we conclude with a call for future research.

# 2. PERSONAS

Personas are archetypal characters who share common goals, attitudes, and behaviors. More specifically, personas can be described as profiles or user models that represent a summation of research data. These fictional characterizations have "names, likenesses, clothes, occupations, families, friends, pets, possessions" [9]. It is these fictional attributes that have influenced the effectiveness of personas [13]. In fact, personas have been used extensively in fields such as marketing and HCI to understand particular users and to inform technology design [4, 5, 8, 20]. Some have used personas to communicate information to a broad range of stakeholders including "designers, developers, testers, writers, managers, marketers, and others" [13].

While some are skeptical about personas [4, 15], there are three main benefits to using personas: they provide focus, improve empathy, and facilitate communication [14]. Specifically, the literature suggests that personas provide a clear understanding of the user audience and allow stakeholders such as technology designers to focus on specific characteristics, needs, goals, and desires of targeted users, which can positively impact technology design [2]. Furthermore, proponents also claim that personas increase empathic feelings toward users. Mulder and Yaar [12], for example, state "personas help you live in your user's shoes...when you face a decision, you might imagine what [persona name] would want to do in this situation, not what you want." This argument suggests that personas increase the emotional connection that designers have with the potential users, allowing for more effective technology design. Although personas are widely used for user-centered design, we suggest personas may also be used to prompt important research questions for further behavioral theory development. Lastly, personas help to clearly and concisely communicate the goals of the users in a way that is consumable. It synthesizes research about users, thereby making communication of the findings of user characteristics easy to consume.

## 2.1 Privacy Segmentation and Personas

Extant research has segmented consumers based on their degree of privacy concern. For example, Westin [10] found that consumers tend to be either unconcerned, pragmatic (i.e., weigh the benefits and protections against the intrusiveness of information sought), or fundamentalist (i.e., generally distrustful of organizations asking for their personal information) in their concern for privacy. Sheehan [16] found support for Westin's typology and defined similar consumer segments based on their degree of privacy concern that included the unconcerned, the circumspect, the wary, and the alarmed. Sheehan's study found the unconcerned consumer to account for 16% of 889 survey respondents.

In building on extant research on privacy concern typologies, we focus on a more granular version of the unconcerned consumer segment whose rationale is if they have not done anything bad, there is no need to hide from or fear data collection. More specifically, we propose developing a persona of the online consumer who subscribes to the NtH perspective. As found in decision-making for user-centered design, we suggest that developing a privacy persona of the NtH consumer can enable privacy scholars to eliminate other issues and focus on the needs of a particular end user as established through the persona [8]. In doing so, we may become better acquainted with this consumer type in order to more clearly conceptualize this consumer's goals and technology usage. In turn, a clearer conceptualization will inform theory development of this consumer's risk behavior, prompt us to consider longer-term implications of unconstrained information disclosure, and aid in more effective PET design.

## 2.2 Dimensions of the 'Nothing to Hide' Persona

In order to further characterize a NtH consumer, we suggest three dimensions: awareness, myopia, and trust. Each dimension is described next.

### *2.2.1 Awareness*

Awareness has been characterized as raised consciousness [19] of data protection problems or solutions. In a separate study by the first author with 269 survey respondents, the 14% of consumers who subscribed to the NtH perspective for online tracking were found to lack awareness of both the methods of and privacy

[1] "Interest-based advertising enables advertisers to reach users based on their inferred interests and demographics (e.g. 'sports enthusiasts')." https://support.google.com/adsense/

protection measures against online tracking. Moreover, awareness of online tracking methods had a strong effect on consumer awareness of tracking-reduction methods.

The NtH consumer has low awareness of the types and pervasiveness of data collection (e.g., with online tracking). That is, a person who subscribes to the 'nothing to hide' perspective does so because he or she does not realize the extent to which personal information is collected. Given low awareness of data collection, the NtH consumer also has low awareness of privacy protection methods.

### *2.2.2 Myopia*

Solove suggested that a NtH person "myopically views privacy as a form of secrecy," not taking into account other threats beyond the potential disclosure of 'bad' things [17]. Additional threats, such as the unintended secondary uses of data collected largely do not occur to the NtH consumer. Secondly, the NtH consumer does not consider the broader possibilities of how a cumulative consumer profile may be used by multiple stakeholders.

Myopic consumers have been studied in other contexts, such as marketing. For example, sellers may condition prices on a consumer's purchasing decisions made during previous site visits [3]. In a study examining when it may be profitable to engage in this form of dynamic pricing, Acquisti and Varian [1] analyzed pricing outcomes for 'myopic' consumers versus 'sophisticated' consumers. In their study, myopic consumers referred to "those who base their purchase decision on the price they see today, not recognizing that the price they face on their next purchase may depend on today's behavior." In contrast, sophisticated consumers referred to those who use anonymizing technologies to avoid establishing a purchase history or delay a purchase.

In general, a myopic consumer bases decisions on the here and now, with less regard for longer-term or broader impacts. The NtH consumer has high myopia.

### *2.2.3 Trust*

Consumers who are not concerned about privacy have been found to be generally trustful of organizations that collect their personal information and are comfortable with organizational procedures and information use [10]. Similarly, research has found consumers are willing to disclose personal information and have that information subsequently used to create consumer profiles for business purposes when they perceive fair procedures are in place [7]. Indeed, voluntary information disclosure largely depends on consumer trust. The NtH consumer exhibits a high degree of trust that data collectors are reputable organizations with legitimate, reasonable intentions (e.g., serve customized ads), that fair procedures are in place, and that justice will prevail in the unlikely event there is impropriety resulting from personal information disclosure.

These three dimensions form a framework from which to construct a NtH persona. The next section presents a fictitious NtH persona for illustrative purposes. Following our example, we discuss how NtH dimensions may be operationalized for theorizing and PET design.

## 2.3 Operationalizing the 'Nothing to Hide' Perspective using Personas

Personas are typically based on interview, observation, and/or survey data [13]. Personas have also been used in conjunction with narrative scenarios as part of user-centered design [9, 11]. We can better evaluate how users' attitudes align with the NtH perspective by conducting interviews or administering a survey instrument containing items that operationalize the three dimensions.

After measuring each dimension, spectrums can be used to further understand study participants [6]. Personas are then created based on participants' placement on the spectrums, thus providing insight on target audiences. These personas can be used to positively impact theory development and technology design.

In analyzing survey responses, researchers can identify patterns on which to base the personas using the dimensions as spectrums [6]. Survey respondents are placed on the spectrums based on their responses to the survey items and in relation to other respondents.

## 2.4 Illustration of a 'Nothing to Hide' Persona

For illustrative purposes, Figure 1 is an example of spectrums based on measures of the three NtH dimensions from a hypothetical sample of survey responses of online consumers. Each survey respondent is represented by a different color. (For large samples of survey respondents, other visualization techniques may be more appropriate such as increasing the size of the circles to illustrate the number of respondents that are the same.)

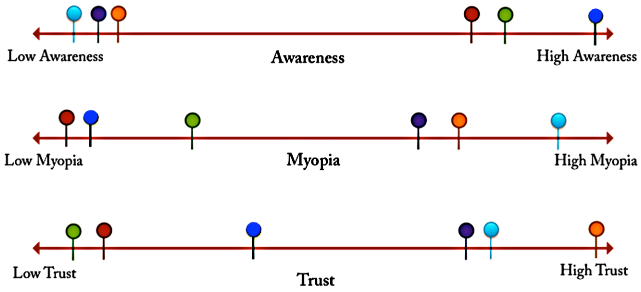


**Figure 1: Spectrums with survey respondents placed in relationship to each other**

Researchers then look for patterns to identify characteristics that are relatively similar. Figure 2, for example, highlights the fact that the respondents represented by light blue, purple, and orange are similar on the three spectrums. Therefore, we could create a persona based on those characteristics. Figure 3 is an example of a fictitious persona, Bryan, derived from the spectrums and demographic items provided by hypothetical survey data and encapsulated in Figure 2.

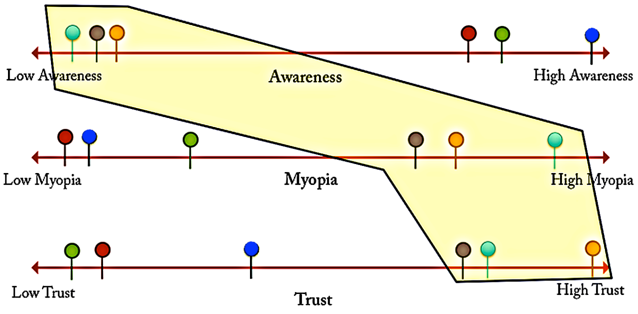


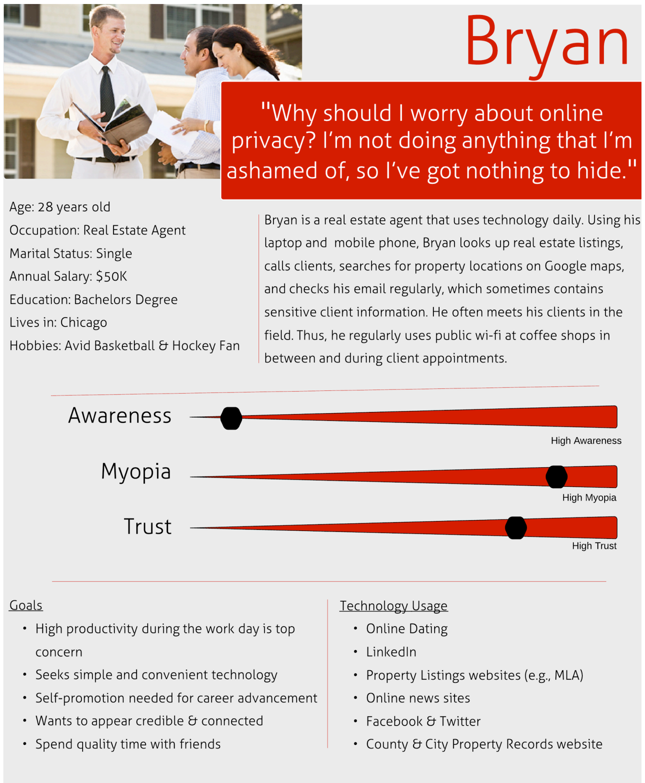
**Figure 2: Spectrum analysis**

In viewing Bryan's goals, technology use, and personal characteristics in Figure 3, we may more clearly conceptualize effective PET design that reaches this consumer archetype. Similarly, we may explore theoretical questions such as how vigilant Bryan may or may not be with using protective measures for his real estate clients' financial and other personal information to which he has access and shares in the context of his work as a real estate agent. For example, given Bryan's low awareness, high trust, and myopic consumerism, how likely is he to use a VPN connection while at coffee shops, alternately viewing client data and visiting dating sites? Given his NtH perspective, goals, and technology usage, how susceptible is Bryan to spyware or spear phishing attacks on the same devices he uses to access and possibly store his clients' data? Given Bryan's low awareness and short time horizon, how likely is Bryan to encrypt or securely delete client data? In other words, is client data more at risk with a NtH consumer like Bryan? With a clearer conceptualization of the risk factors involved in Bryan's NtH persona, how can PET tools be more effectively designed?

Researchers may also be interested in studying the vast profile a NtH consumer like Bryan accumulates over time. Given his tendency to freely self-disclose across various social networking sites, thus leaving behind a more complete profile than consumers with higher privacy concern, is he more or less at risk for information distortion? Thus, the visual and contextual detail of Bryan's NtH persona compels us to more vividly see privacy risk factors in Bryan's environment. This clearer conceptualization prompts us to ask relevant and important research questions that can positively influence public policy and technology design.

## 3. CONCLUSIONS AND FUTURE RESEARCH

Daniel Solove [17] introduced the concept of a NtH perspective of privacy regarding one's response to government surveillance (e.g., NSA surveillance programs) for the sake of national security. We suggest that the NtH perspective applies equally to commercial collection of online consumer information for the sake of interest-based advertising. In both contexts, those who subscribe to the NtH perspective of privacy generally believe that if one is not doing something wrong, then one has nothing to hide, and so has nothing to fear (i.e., has no need to worry) about pervasive data collection of day-to-day online browsing, transactions, or communication.



Bryan

"Why should I worry about online privacy? I'm not doing anything that I'm ashamed of, so I've got nothing to hide."

Age: 28 years old
Occupation: Real Estate Agent
Marital Status: Single
Annual Salary: $50K
Education: Bachelors Degree
Lives in: Chicago
Hobbies: Avid Basketball & Hockey Fan

Bryan is a real estate agent that uses technology daily. Using his laptop and mobile phone, Bryan looks up real estate listings, calls clients, searches for property locations on Google maps, and checks his email regularly, which sometimes contains sensitive client information. He often meets his clients in the field. Thus, he regularly uses public wi-fi at coffee shops in between and during client appointments.

Goals

- High productivity during the work day is top concern
- Seeks simple and convenient technology
- Self-promotion needed for career advancement
- Wants to appear credible & connected
- Spend quality time with friends

Technology Usage

- Online Dating
- LinkedIn
- Property Listings websites (e.g., MLA)
- Online news sites
- Facebook & Twitter
- County & City Property Records website

**Figure 3. Example of a 'Nothing to Hide' persona**

The NtH perspective raises new and scarcely explored research questions on the implications of this privacy perspective. Creating a NtH persona is a first step in more fully conceptualizing this consumer segment. A NtH persona prompts us to ask research questions about how someone with this privacy perspective may behave or use technology, and thus lays a foundation from which to theorize and influence PET design for this particular consumer segment.

There are several opportunities for future research. First, although NtH has been discussed in insightful, practical terms [17], theory development and empirical validation are needed in order to more fully understand this perspective and its implications for consumers, public policy makers, and PET designers. While this paper proposes three dimensions of the NtH consumer based on extant research, further development and validation is needed. Moreover, theorizing the risk behavior of a NtH consumer could inform organizational security measures, public policy, and technology design. Second, few have discussed standards by which personas should be created, specifically for the area of privacy. Applying insights from HCI researchers and practitioners who have used personas extensively for technology design, privacy scholars can develop best practices to design privacy personas that are not only effective but that also provide focus, facilitate communication, and increase empathy. Third, the Symposium on Usable Privacy and Security (SOUPS) workshop on privacy personas and segmentation suggests there are new concepts that have yet to be operationalized and could be conceptualized through personas, such as the NtH perspective toward privacy. Future research can explore other consumer segments, such as the fundamentalist [10] who has a basic mistrust of information requesters.

## 4. REFERENCES

[1] Acquisti, A. and Varian, H. R. Conditioning Prices on Purchase History. Marketing Science, 24( 3), 2005, 367–381.

[2] Adlin, T., Pruitt, J., Goodwin, K., Hynes, C., McGrane, K., Rosenstein, A. and Muller, M. J. Putting personas to work. ACM, CHI Extended Abstracts, 2006.

[3] Aloysius, J., Deck, C. and Farmer, A. Sequential Pricing of Multiple Products: Leveraging Revealed Preferences of Retail Customers Online and with Auto-ID Technologies. Information Systems Research, 24(2), Jun 2013, 372–393.

[4] Blomquist, Ö. and Arvola, M. Personas in action: ethnography in an interaction design team. ACM, Nordic Conference on HCI, 2002.

[5] Cooper, A. The inmates are running the asylum: Why high-tech products drive us crazy and how to restore the sanity. Sams Indianapolis, 1999.

[6] Cooper, A., Reimann, R. and Cronin, D. About face 3: The Essentials of Interaction Design. Wiley Publishing, Inc, Indianapolis, 2007.

[7] Culnan, M. J. and Armstrong, P. K. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 10(1), 1999, 104-115.

[8] Friess, E. Personas and decision making in the design process: an ethnographic case study. CHI, ACM, 2012.

[9] Grudin, J. and Pruitt, J. Personas, participatory design and product development: An infrastructure for engagement. PDC, 2002.

[10] Kumaraguru, P. and Cranor, L. F. Privacy Indexes: A Survey of Westin's Studies. Carnegie Mellon University, Report CMU-ISRI-5-138, 2005.

[11] Lewis, M. M. and Coles-Kemp, L. Who says personas can't dance?: the use of comic strips to design information security personas. ACM, CHI, 2014.

[12] Mulder, S. and Yaar, Z. The user is always right: A practical guide to creating and using personas for the web. New Riders, 2006.

[13] Pruitt, J. and Grudin, J. Personas: practice and theory. ACM, Conference on Designing for User Experiences, 2003.

[14] Putnam, C. Bridging the Gap between User Experience Research and Design in Industry: An Analysis of Two Common Communication Tools--Personas and Scenarios. ERIC, 2010.

[15] Rönkkö, K., Hellman, M., Kilander, B. and Dittrich, Y. Personas is not applicable: local remedies interpreted in a wider context. ACM, Conference on Participatory Design: Artful integration: interweaving media, materials and practices, 2004.

[16] Sheehan, K. B. Toward a Typology of Internet Users and Online Privacy Concerns. The Information Society, 18, 2002, 21-32.

[17] Solove, D. J. Nothing to Hide: The False Tradeoff between Privacy and Security. Yale University Press, New Haven, 2011.

[18] Solove, D. J. Why privacy matters even if you have 'nothing to hide'. The Chronicle of Higher Education, 57(37), May 20 2011.

[19] Spears, J. L. and Barki, H. User Participation in IS Security. MIS Quarterly, 34(3), Sep 2010, 503-522.

[20] Wärnestål, P., Svedberg, P. and Nygren, J. Co-constructing child personas for health-promoting services with vulnerable children. ACM, Conference on Human Factors in Computing Systems 2014.