

**Privacy Norms And The Consumer Exchange Relationship Online: The Impact Of
Consumer Tracking And Targeted Advertising On Trust And Willingness To Engage.**

Kirsten Martin, Ph.D.
George Washington University
School of Business

DRAFT – PLEASE DO NOT CITE WITHOUT CONTACTING AUTHOR

Submitted to FTC PrivacyCon

October 2016

Privacy Norms And The Consumer Exchange Relationship Online: The Impact Of Consumer Tracking And Targeted Advertising On Trust And Willingness To Engage.

ABSTRACT

Online websites regularly engage with data aggregators and ad networks to support behaviorally targeted advertising, yet little is known about whether and how information used for online advertising fits within the norms of the consumer exchange online. Two alternative approaches to privacy norms within the marketing exchange predict divergent hypotheses about consumer trust and behavior. A series of studies examines the scope and relative importance of privacy norms presumed in the marketing exchange relationship to consumer trust and engagement. The results demonstrate that non-contextual, secondary use of information is considered outside the marketing exchange norms and a violation of trust. In fact, the results show that selling information to an ad network is considered on par with the security violation of a hacker stealing information in violating trust. In addition, an experiment shows respondents are less willing to engage with a partner violating privacy norms of the marketing exchange by utilizing pervasive tracking. These studies illustrate how the interests of consumer-facing firms, who maintain an important exchange relationship with consumers, may not be aligned with the interests of ad networks and data aggregators who benefit from pervasive consumer tracking and data monetization.

Keywords: consumer trust, online marketing, valuation of privacy, behavioral targeted advertising.

Privacy Norms And The Consumer Exchange Relationship Online: The Impact Of Consumer Tracking And Targeted Advertising On Trust And Willingness To Engage.

Targeted marketing online necessitates a robust picture of the consumer through ubiquitous tracking, and an information ecosystem comprised of data aggregators, data brokers, trackers, websites, and ad networks collects and stores consumer information online. To support the \$49.5B industry of online advertising (Urbanski, 2014), the FTC reported that top data aggregators covered over 80% of the U.S. population and could identify vehicle ownership, buying behavior, medical purchases, consumer finances, charitable donations, and even what consumers watched (2014). Consumer tracking is considered critical to industry online (Hoffman, Novak, and M. Peralta 1999) and specifically for behaviorally targeted advertising (Acquisti, Brandimarte, and Loewenstein 2015; Tucker 2015, 2014).

One set of actors consistently benefiting from consumer tracking and behaviorally targeted advertising are data aggregators and ad networks who play the intermediary between companies looking to advertise their product and the publisher (the consumer-facing website). Advertising firms can charge higher rates for behavioral targeted ads versus run-of-network or banner ads (Beales 2010). The revenue for ads increases by 60% for those with cookies (with tracked information) versus those without cookies and as much as 200% for cookies with more information (Beales and Eisenach 2014). Across types of consumer information collected, ad networks and data aggregators consistently benefit from tracking consumers (Marotta, Zhang, and Acquisti 2015).¹

¹ The benefit of consumer tracking and associated targeted advertising to the advertisers promoting their products is not as clear. When advertising must rely on contextual rather than behaviorally targeted advertising due to new regulations, consumer purchasing intent decreases for advertising on general websites but not for specific content websites (Goldfarb and Tucker 2011). Advertisers find value in behavioral advertising as a channel substitute; firms are willing to pay more for targeted ads when regulations preclude them from contacting consumers directly

Yet, the tracking of consumer information is increasingly the subject of consumer concerns. Tactics integral to the online marketing ecosystem – consumer tracking, behavioral targeting, retargeting – are deemed privacy violations by popular and academic surveys (Leon et al. 2015; Martin 2015a; Martin and Shilton 2015; Turow et al. 2009; Ur et al. 2012). These privacy concerns drive consumers’ general feeling of information risk, vulnerability, and decreasing trust online (Pew Research Center 2014a; b; Turow, Hennessy, and Draper 2015). As noted by Tucker, “The unusual feature of online advertising markets is that they are characterized by a tension between the desire of a firm to be informative to the right set of consumers, and consumers’ apparent distaste for how firms use data...” (Tucker 2012).

One party particularly vulnerable to an adverse consumer reaction is consumer-facing publishers (NYTimes, ESPN, WebMD, etc) who display the behaviorally targeted ads and facilitate the tracking of user behavior online. Consumer firms online rely on understanding and respecting the consumers’ marketing exchange relationship to ensure their policies and practices engender trust. And, the norms of the exchange act as guidelines for consumers and firms (Cropanzano and Mitchell 2005). The marketing exchange online, whereby consumers engage with a firm while balancing the associated costs and benefits, is the critical subject of economics, public policy, and marketing to ensure effective governance of the exchange. The exchange is the subject of regulations and the FTC (Martin 2015a), and adequate notice at the time of the consumer disclosing information is the primary vehicle to governing the exchange (Martin 2013; Solove and Hartzog 2014).

Recent consumer backlash and surveys calls into question the presumed approach to privacy norms within this consumer exchange. As summarized by Martin and Murphy in an

(Goldfarb and C. Tucker 2011a). However dynamic retargeting, where a consumers’ online behavior dictates the advertising seen later online, was found to be less effective in purchasing intent (Lambrecht and Tucker 2013).

analysis of data privacy and marketing, firms “have responded as though they were granted access to personal information and permission to disclose, currently capturing, storing, and selling vast amounts of consumer data (Singer 2012)” (Martin and Murphy forthcoming). While firms remain focused on the presumed norms of the marketing exchange relationships, consumers consistently express concern about how information is gathered, shared, and used online. The benefits of consumer tracking and associated behavioral targeting for both firms advertising their products as well as ad networks and data aggregators continues to be studied, yet less research has attempted to examine the limits of the privacy norms driving consumer marketing exchange online.

The goal of this paper is to empirically examine the privacy norms of the marketing exchange relationship online and measure their relative importance to consumer trust and a consumers’ willingness to engage with a firm. We develop and then test hypotheses based on two approaches to privacy norms – privacy as that which remains controlled or inaccessible to others and privacy as that when information is accessed, used, and shared in context-appropriate manner (Martin 2015b; Nissenbaum 2010)– within the customer marketing exchange. A series of four factorial vignette surveys were used to identify the privacy norms presumed in consumers’ marketing exchange online. Respondents rated websites in a series of realistic online scenarios as to the degree of trust in the website. Subsequent analysis identified the relative importance of costs and benefits of using customer information in the marketing exchange. An experiment then quantifies the impact of respecting privacy norms of the marketing exchange on consumers’ willingness to engage with a partner such as a website.

Here, we use the role of norms in social exchange theory as guidelines for appropriate behavior and developing mutual trust in exchange relationships. Privacy norms, we argue below,

are an important normative guideline for marketing exchange relationships when online and respecting privacy norms builds consumer trust – as with norms and social exchange theory more generally (Cropanzano and Mitchell 2005). Further, the formation of trust is key for a consumer’s “willingness to engage in an exchange relationship” at the level of vulnerability required online (Johnson and Selnes 2004, p. 4).²

Consumers’ perception of privacy norms online are difficult to measure. Previous studies have focused on proxies for privacy-respecting and privacy-violating behavior as shown in Table 1. The existence of a third-party seal (Bart et al. 2005; Belanger, Hiller, and Smith 2002a), adequate notification (Miyazaki and Fernandez 2000; Roman 2007), or the respondents’ belief of a given websites’ practices (Riquelme and Román 2014; Roman 2007) have served as approximate measures of whether consumers find the use of data appropriate online. Notice and seals are notoriously ill-suited to explain the actual information flows between firms and the marketing ecosystem of ad networks, data aggregators, data brokers, etc.

The factorial vignette survey methodology and this study design offer three unique contributions. First, rather than using a proxy, such as the degree of website notification or the presence of a privacy seal, the vignettes operationalize primary and secondary uses of information with specific, tested practices to analyze the impact on consumer trust. Consumer behavior does not necessarily bely their privacy preferences due to the high information asymmetry in regards to actual firm privacy practices (Martin 2013). Second, the vignettes include both benefits of the marketing exchange as well as the possible costs and risks in information use. The respondent is able to weigh the ‘tradeoff’ in the vignette rating. Finally, the

² Consumer trust, as the willingness to be vulnerable based on perceptions of the reliability and integrity of a firm (Garbarino and Johnson 1999; Mayer, Davis, and Schoorman 1995), is key for increasing purchase intentions (Lee

trust game experiment measures actual respondent behavior as a willingness to engage rather than trust judgments or intent.

The results show that the privacy norms of the marketing exchange relationship are consistent with privacy as the contextually appropriate use of information: consumers judged the contextual, primary use of information as within the exchange but the secondary, non-contextual use of information to be outside the exchange and a violation of trust. Further, and consistent with privacy as the contextually appropriate use of information, the secondary uses of information – such as selling consumer information to data aggregators and targeting friends – are considered on par with a security violation of an outsider (i.e., a hacker) stealing information from a website.

In addition, the results demonstrate that respecting privacy norms is important to consumers' economic behavior. The trust game experiment shows respondents are less willing to engage with a partner who violated privacy norms of the exchange relationship and utilized pervasive tracking. Importantly, breaching the privacy norms of the marketing exchange by using an ad network leads more consumers to chose a competitor or walk away from a website particularly for individuals with moderate and low institutional trust.

This study has implications for the relationship between consumer-facing firms and data driven online marketing firms online. The interests of the larger online marketing ecosystem – including data aggregators, data brokers, ad networks – to gather, aggregate, and sell personally identifiable information may not align with the interests of firms to develop the consumer relationship and maintain consumer trust. While data aggregators, data brokers, and ad networks benefit from highly personalized and aggregated consumer data (Beales 2010; Marotta, Zhang,

and Acquisti 2015), publishers with an existing relationship with consumers may not benefit enough to counter consumers' decrease in trust and willingness to engage.

For firms, if consumers perceive online marketing tactics, such as selling information to a data aggregator, outside the norms of the exchange, then marketers online could face a consumer backlash once the practices are known. Marketers could limit the use of personal information shared and used for marketing as research has illustrated the limits in effectiveness of personalized marketing tactics online (Lambrecht and Tucker 2013). The benefits of contextual-targeting based on content rather than tracked information (Goldfarb and C. Tucker 2011b) and privacy preserving targeted ads (Toubiana et al. 2010) would fit within the established need to selectively use targeted advertising for economic reasons (Iyer, Soberman, and Villas-Boas 2005).

Table 1: Review of Previous Research on Privacy, Security, and Trust

<i>Source</i>	<i>Privacy as..</i>	<i>Security as...</i>	<i>Operationalized for Respondent</i>
<i>Measuring presence of third party seal</i>			
(Lee and Turban 2001)	Certification bodies	Certification bodies	Existing third-party recognition bodies are adequate for the protection of Internet shoppers' Interest; I think third-party recognition bodies are doing a good job.
(Belanger, Hiller, and Smith 2002b):	Privacy seals and statements	Security seals	How important are ___ in your decision to buy on the World Wide Web?" (1) third party privacy seals, (2) privacy statements, (3) third party security seals, and (4) security features)....
(Bart et al. 2005)	n/a	Seals (e.g., TRUSTe or Verisign) presence.	There were signs or symbols on the site placed there by third-party companies indicating that the site had been reviewed or audited for sound business practices; There were trust seals present (e.g., TRUSTe); There were seals of companies stating that my information on this site is secure (e.g., Verisign);
<i>Measuring adequate notification</i>			
(Roman 2007)	Easy to understand policy	Easy to understand policy	Security policy is easy to understand; Site displays the terms and conditions of the online transaction before purchase has take place; Information regarding the privacy policy is clearly presented
(Miyazaki and Fernandez 2000)	Degree of disclosure	Degree of disclosure	The authors examine online retailer disclosures of various privacy- and security-related practices
(Bart et al. 2005):	Ease to find/ understand policy	n/a	The general privacy policy is easy to find on the site; The text of the privacy policy is easy to understand; Information regarding security of payments is clearly presented; Informational text regarding the site's use of cookies is clearly presented
<i>Measuring features perceived by respondent after visiting site</i>			
(Kim 2005):	Concern about perceived practices	Perception of website's tactics	This web vendor implements security measures to protect internet shoppers; this web vendor has the ability to verify internet shoppers identities for security purposes; I am concerned that this website is collecting too much personal information about me; I am concerned that this web vendor will use my (or share my) personal information for other purposes without my authorization.
(Flavián and Guinalíu 2006)	Perception of website's concern	Perception of website's actions	I think this website shows concern for the privacy of its users; I think this website abides by laws.
(Kim, Ferrin, and Rao 2008).	Perceived privacy protection:	Perceived security protection:	I am concerned this website is collecting too much personal information from me...this website will use my personal information for other purposes without my authorization; This web vendor implements security measures to protect internet shoppers. I feel safe in making transactions on this website....
(Cheung and Lee 2006)	Perceived privacy control	Perceived security control	Internet vendors implement security measures to protect internet shoppers...have the ability to verify internet shoppers identify for security purposes; I am concerned for my privacy; e.g., Internet vendors' concern about consumers' privacy...will sell my personal information ...
(Mukherjee and Nath 2007)	Perceived Privacy features	Perceived Security Features	The online retailer does not divulge or sell customer information without the customer's consent; The customer does not receive unsolicited emails from this online retailer; The security features used by the online retailer are latest; The customer's credit card information is not prone to leakage; The online retailer has not been hacked in the past.

RELATED SCHOLARSHIP AND HYPOTHESES DEVELOPMENT

Consistent with social exchange theory generally, marketing exchange relationships are evaluated based on the expected benefits and costs to each party: customers choose firms that provide the greatest net benefits minus any expected costs (Johnson and Selnes 2004). A basic premise of social exchange theory is that relationships vary from arms-length to ones with greater trust and commitment. And several theories of relationship marketing propose that customers vary in their relationships with a firm on a continuum from transactional to highly relational bonds (Garbarino and Johnson 1999; Hill and Martin 2014).

Online, consumers enter into a relational exchange rather than a more transaction exchange almost immediately due to the level of consumer information gathered and the associated consumer risk, vulnerability and required trust. Trust has long been considered critical online due to the lack of an actual face-to-face relationship with consumers (Hoffman, Novak, and M. Peralta 1999; Kim, Ferrin, and Rao 2008). Trust, as the willingness to be vulnerable based on perceptions of the reliability and integrity of another (Garbarino and Johnson 1999; Lee and Turban 2001; Schlosser, White, and Lloyd 2006), is seen as necessary for consumers to disclose information online (Chellappa and Sin 2005; Milne and Boza 1999).

Not surprisingly, privacy – as the norms about how information will be gathered, used, and shared – becomes increasingly important to marketing exchange relationships online. Social exchange theories can differ as to the types of norms of fairness or reciprocity expected in the exchange relationships, and abiding by the norms of the exchange acts as important guidelines of appropriate behavior as parties move to more trusting relationships (Cropanzano and Mitchell 2005). Consumers and firms manage information risk within exchange relationships as to the privacy norms about how information is gathered, used, shared.

Examining privacy as within a marketing exchange or exchange relationship is not new (Culnan and Bies 2003); scholars examine consumers revealing personal information when perceived benefits outweigh perceived costs within marketing (Schumann, von Wangenheim, and Groene 2014; White, Novak, and Hoffman 2014). With pervasive flows of consumer information across all exchange relationships online, consumers trust firms to respect the ‘terms of use’ around information – or the implicit social contract around how the information is gathered and used and shared (Culnan and Bies 2003; Liu et al. 2014).

Privacy norms are critical to a relational exchange online where norms and trust are central (Sirdeshmukh, Singh, and Sabol 2002; Vargo and Lusch 2004), yet the definition or scope of privacy norms remains ambiguous within the marketing exchange (Martin and Murphy forthcoming; Martin 2015b). The consumer exchange relationship currently relies on a handoff of consumer information where voluntary disclosure is equated with less privacy expected – thus allowing firms to use information for online marketing (Martin and Murphy 2016). Online, individuals are framed as unconcerned or willing to trade privacy (Westin 2001, 2003). Alternatively context-dependent definition of privacy – privacy as a social contract (Martin 2015b) or privacy as contextual integrity (Nissenbaum 2010) – posit individuals as approving of the contextual use of their information but find the non-contextual secondary use to be a violation. Both approaches to privacy predict different judgments and reactions of consumers to the use of information for marketing below.

Scope of privacy norms in exchange relationships online

Privacy online is frequently framed as hinging on voluntary disclosure of information as a critical inflection point. Specifically consumers are viewed as relinquishing their privacy rights

or having diminished privacy expectations for receiving compensation when engaging online (Gabisch and Milne 2014; Hui, Teo, and Lee 2007; Sheehan 2005; Westin 2003). The justifications for relinquishing privacy interests are diverse: consumers are willing to disclose information for personalization (Xu et al. 2009) as well as free services and useful ads (Banerjee and Dholakia 2008).

The focus on consumers' disclosure of information online as the equivalent of a handoff of information and privacy interests is supported by two popular definitions of privacy. Both privacy as that which is inaccessible (Warren and Brandeis 1890) and privacy as that which is controlled (Milne and Culnan 2004; Sheehan and Hoy 2000) support disclosure as the critical point where information is no longer private as if disclosing information is equivalent to handing over ownership to another party with the associated rights due to less control or due to making information accessible (Gabisch and Milne 2014; Milne and Gordon 1993).

And the approach to privacy norms whereby individuals relinquish privacy interests when online dominates practice and public policy. The FTC's focus on adequate notice rather than minimum standards of information protection reinforces disclosure as handing over ownership of information (Norberg, Horne, and Horne 2007; Teufel 2008), and the belief that disclosed information is public strengthens an 'anything goes' approach to information privacy (Martin and Nissenbaum 2016; Nissenbaum 2004; Zimmer 2010).

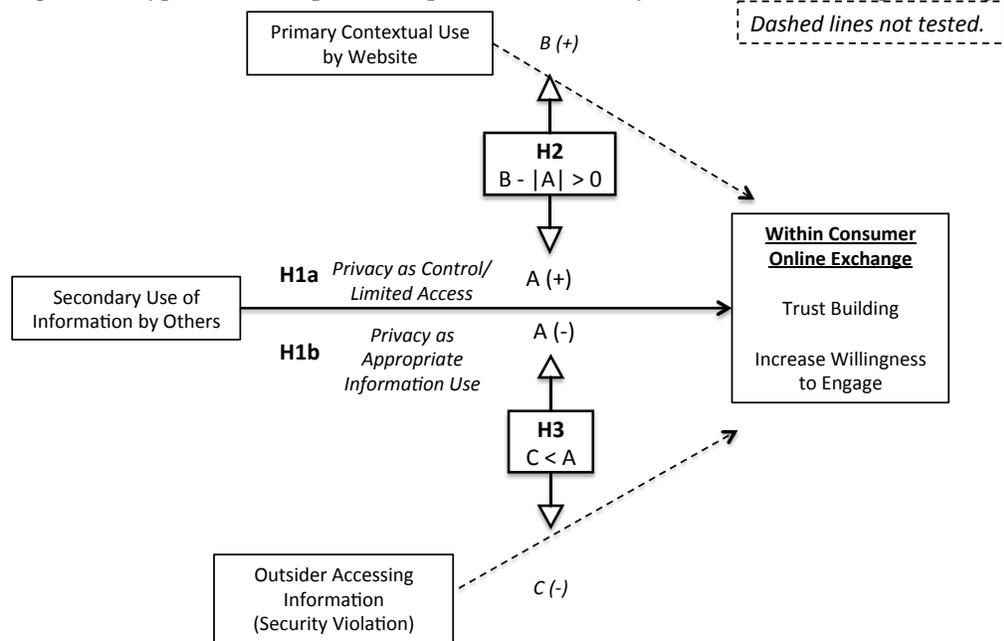
The use of pervasive tracking to support hyper targeted advertising relies on the premise that such practices are within consumers' exchange relationship with the publisher online (Schumann, von Wangenheim, and Groene 2014) and that consumers would have agreed to pervasive tracking with a general social contract if given a chance (Dunfee, Smith, and Ross Jr 1999; Martin 2015b). Consumers are seen as pragmatic or unconcerned about the use of their

information and privacy in general (Westin 2003). Privacy norms of the marketing exchange online presumes the consumer relinquished privacy expectations around the future use of information when the consumer made the information accessible to the website.

H1a: The use of information online by additional actors and future uses will be judged to be within the consumers’ marketing exchange relationship online and, therefore, not impact consumer trust in the website.

[Figure 1 about here]

Figure 1: Hypotheses: Scope and Importance of Privacy Norms in Marketing Exchange Relationship



Alternatively, privacy as contextually dependent – such as privacy as contextual integrity (Nissenbaum 2010) and privacy as a social contract (Martin 2015b) – suggests individuals have expectations about the type of information that is accessed by an actor and subsequently used for a given community. Privacy violations, therefore, are the breaches of these norms – when the type of information is given to the wrong person or used in an inappropriate way (Martin 2015).

Importantly, context dependent approaches place no special focus on disclosure or sharing data as suggestive of less privacy – appropriate norms of information flow would always apply no matter who has access or where the information is shared.

However, using information in a new context with new actors and for new purposes may violate consumers' norms of appropriate use (Nissenbaum 2010). When the type of information is given to the wrong actor or used in an inappropriate way, the privacy norms are said to be violated or breached (Martin 2015). In other words, how websites gather, store, share, and then use information online are subject to privacy norms; consumers have privacy concerns and perceive violations of privacy when information is shared, stored or used in a manner deemed inappropriate for that particular context. Previous work has identified the secondary use of information as a privacy concern (Belanger, Hiller, and Smith 2002b; Flavián and Guinaliú 2006) and consumers clear concerns about the secondary use of information for data brokers and marketing (Martin 2014; Pew Research Center 2014; Rainie et al. 2013; Turow, Hennessy, and Draper 2015)

Therefore, where the dominant approach to privacy norms online relies upon consumers as having no privacy expectations about with whom the information is shared and how information is used within the general online advertising eco system, privacy as contextually dependent suggests consumers will judge sharing with second parties and using data outside the immediate context to be a violation of the privacy norms of the consumer exchange relationship.

H1b: The use of information online by additional actors and future uses will be judged to be outside the consumers' marketing exchange relationship online and, therefore, negatively impact consumer trust in the website.

Importance of privacy norms to exchange relationships online

Public surveys capture consumers' grave concern over privacy online, yet many also note the relative importance of respecting privacy to the consumer exchange relationship is not as clear. While consumers may express concerns about marketing online or even find pervasive tracking a violation of the privacy norms as hypothesized in H1b, the oft-reported privacy paradox, whereby individuals report a general concern about privacy yet continue to share information (Pavlou 2011; Smith, Dinev, and Xu 2011; Xu et al. 2011), suggests that respecting privacy norms may be important but need to be put into perspective to (a) the possible benefits of being online and (b) the larger harms and risks when online. Both alternatives are explored below.

Tracking consumer information, according to the marketing exchange, is the necessary cost of going online within a broad consumer marketing exchange online. Practitioners and scholars suggest that consumers knowingly take on certain risks in disclosing information in order to benefit from targeted advertising, personalized online experience, and free content. Accordingly, information flows deemed privacy violations in consumer surveys may be better judged when taking into consideration the benefits of sharing information online.³ Consumers receive benefits such as “customized offerings, personalization value, streamlined customer–firm interactions, access to free services, and even financial compensation” (Martin and Murphy forthcoming). While consumers may be vulnerable to the later misuse of tracked and aggregated data (Calo 2011; Crawford 2013; Crawford and Schultz 2014; Richards and King 2014), consumers are willing to provide their information in exchange for benefits (Schumann et al. 2014).

³ Here the term ‘consumers disclose information’ insinuates a form of intentional disclosure of information online. Consumers more accurately merely interact with a website or mobile application without any knowledge, let alone intentionality, around the type of information exposed.

According to the exchange, “users benefit from a free service and are willing and motivated to collaborate” by sharing information (Schumann, von Wangenheim, and Groene 2014, p. 66). The exchange has empirical support in that consumers keep mental accounts of the costs and benefits of the sharing information (White, Novak, and Hoffman 2014). Consumers take into consideration the risks and benefits of disclosing information when assessing privacy concerns and expectations (Culnan and Bies 2003; Dinev and Hart 2006; Hui, Teo, and Lee 2007; Xu et al. 2009).

H2: Regardless of the norm of privacy, consumers perceive the benefits of sharing information to outweigh any perceived harms and risks

Just as the beneficial uses of information help put into perspective the importance of privacy norms to consumers in H2 above, comparing the importance of violating privacy norms to clear violations of the marketing exchange relationship can place a lower bound on the relative importance of violating privacy norms to consumers online. Security violations are similar to privacy violations as both introduce greater information risk and render consumers vulnerable to possible harms (Dinev and Hart 2006; Milne and Culnan 2004; Youn 2009).⁴ Yet, where privacy violations are actions the firm takes to treat consumer information inappropriately, security violations are outsiders (e.g., hackers) who cause harm by damaging a system or accessing, disclosing, and misusing consumer data (Belanger, Hiller, and Smith 2002b; Flavián and Guinaliú 2006; Miyazaki and Fernandez 2000).

Consumer concerns about security of their data has only solidified in recent years with well known cyber attacks such as Target, the New York Times, and even the Office of Personnel

⁴ Privacy and security are defined and treated as distinct concepts similar to previous scholars (Belanger, Hiller, and Smith 2002b; Lee and Turban 2001; Miyazaki and Fernandez 2000, 2001; Riquelme and Román 2014; Roman 2007; Román and Cuestas 2008) – rather than conflated into one construct as a single source of vulnerability for consumers (Flavián and Guinaliú 2006; Lee and Turban 2001; Schlosser, White, and Lloyd 2006).

Management (OPM) in 2015. A growing number of consumers raise cyber security as a main concern with 50% of respondents in 2014 from 33% in 2009 (Pew Research Center 2014b). Experts agree that cyber security attacks are likely to increase in frequency and scope (Pew Research Center 2014c).

And, security violations have become the focus of public policy. Firms' consumer information security practices are increasingly the subject of government scrutiny through the FTC as well as through regulations of specific industries such as FINRA and HIPPA. Security is not only a regulatory issue with the U.S. Congress proposing the Data Security Act of 2015 to set minimum standards for the security of consumer data from outside access. The SEC has elevated the issue of cybersecurity to the level of the board of directors of public companies to maintain the integrity of the markets (Aguilar 2014).

While surveys have shown the relationship between security and privacy concerns of consumers (Pew Research Center 2014a), the risks to the consumer as evidenced by regulators' attention and standards of practice would be substantially greater for security violations as compared to privacy norm violations.⁵ Therefore, security violations would constitute a lower bound on violations of the norms of the marketing exchange relationship as we would expect, when directly asked, consumers would judge security violations to be well outside the norms of the marketing exchange relationship.

H3. Regardless of the norm of privacy, security violations will be significant larger threats to the norms of the marketing exchange relationship online and, therefore, have a significantly larger negative impact on consumer trust in the website compared to a violation of privacy norms.

⁵ Consumers may not realize how intertwined trackers and targeted ads are with security concerns: ad networks have recently been used to install ransomware on consumers' computers by hackers (Trimm 2016).

Importance of privacy norms to willingness to engage

Experiments have been effective to capture consumers' preferences and the relative importance of particular information practices to actual consumer behavior (Acquisti, Brandimarte, and Loewenstein 2015). Through experiments, consumers' willingness to disclose have been shown to be based on their familiarity with the other party (John, Acquisti, and Loewenstein 2011) and the relative standards of disclosure behavior (Acquisti, John, and Loewenstein 2012). In addition, Grossklags and Acquisti identify and measure the important difference between consumers' willingness to accept (WTA) current privacy practices about how information is gathered, used, stored, and shared versus consumers' willingness to pay (WTP) for privacy to be respected in a certain manner (Grossklags and Acquisti 2007). Both WTA and WTP capture an amount (e.g., \$0.25) consumers would pay to retain or purchase privacy protection illustrating behavioral economic concepts such as loss aversion.

Voluntary disclosure, WTA, and WTP each presupposes a consumers willingness to engage with a transaction partner. In other words, how much would someone pay (WTP) assuming they still do business with the other party. However, many publishers do not have a revenue model based on consumer payment and rely on engagement as a measure of success. In addition, with low switching costs for initial purchases, a consumer could walk away from a website online and disengage before accepting or being willing to pay. If consumers are not willing to engage and chose a competitor instead, the firm would not be able to even promote their products or fine-tune their tracking and targeting practices to market to consumers.

H4: Practices outside the privacy norms of the marketing exchange will negatively impact consumers' willingness to engage with a partner.

[Table 2 about here]

Table 2: Hypotheses and Analysis

	<u>Concept Tested</u>	<u>Concept Explained</u>	<u>Analysis in Results</u>
H1a	<i>Privacy as Control/Limited Access</i>	Privacy norms of the marketing exchange relationship online presumes the consumer relinquished privacy expectations around the future use of information when the consumer made the information accessible to the website. H1a: <i>The use of information online by additional actors and future uses will be judged to be within the consumers' marketing exchange relationship online and, therefore, not impact consumer trust in the website.</i>	The coefficient of the secondary use of information will be positive or not significant; secondary use of information will have a positive or insignificant impact on trust and/or a willingness to engage
H1b	<i>Privacy as Appropriate Information Use</i>	Privacy norms of the marketing exchange relationship online includes whether the information is used in a contextually appropriate manner. H1b: <i>The use of information online by additional actors and future uses will be judged to be outside the consumers' marketing exchange relationship online and, therefore, negatively impact consumer trust in the website.</i>	The coefficient of the secondary use of information will be negative; secondary use of information will have a negative impact on trust and/or a willingness to engage
H2	<i>Marketing Exchange</i>	H2: <i>Regardless of the norm of privacy, consumers perceive the benefits of tracking to outweigh any perceived harms and risks</i>	The importance of primary, contextual use will outweigh (be greater than) any perceived costs of the secondary use of information for marketing. With both costs and benefits being taken into account, the consumer trust in the firm will be positive.
H3	<i>Limit of Marketing Exchange</i>	H3: <i>Regardless of the norm of privacy, security violations will be significant larger threats to the norms of the marketing exchange relationship online and, therefore, have a significantly larger negative impact on consumer trust in the website compared to a violation of the privacy norm</i>	The importance of violating privacy norms through the secondary use of information will be significantly less than the importance of security violations by outside parties.
H4	<i>Importance to Privacy Norms to Economic Activity</i>	H4: <i>Practices outside the privacy norms of the marketing exchange will negatively impact consumers' willingness to engage with a partner.</i>	The percent of respondents willing to engage with a partner who violates privacy norms will be significantly lower than the percent willing to engage with a partner respecting privacy norms.

OVERVIEW OF STUDIES

The goal of the paper is to empirically examine the scope and relative importance of privacy norms in the marketing exchange relationship online. To this end, the factorial vignette survey methodology was used to test the privacy norms around tracking users and behaviorally targeted advertising in consumers' marketing exchange. Factorial vignette survey methodology was developed to investigate human judgments using highly contextual vignettes (Jasso 2006b; Rossi and Nock 1982; Wallander 2009b). In a factorial vignette survey, a set of vignettes is generated for each respondent, where the vignette factors are controlled by the researcher and randomly selected, and respondents are asked to evaluate each hypothetical situation with a single rating task.

The vignettes allow the respondent to see realistic scenarios and judge the degree of trust or distrust in the website. The methodology is designed to avoid respondent bias where respondents attempt to answer surveys in a manner that is socially desirable. Importantly, the factorial vignette methodology enables researchers to simultaneously examine multiple factors – e.g., the benefits and possible harms of the marketing exchange (Johnson and Selnes 2004) – using vignettes which are systematically varied (Ganong and Coleman 2006).

In Surveys 1-4 using factorial vignette survey methodology, the respondents were prompted to rate the degree to which they trusted the website in the vignette, and statistical techniques were used to identify the relative importance of each vignette factor in driving the respondents' trust rating. The surveys were deployed over the course of 3 months through

Amazon’s Mechanical Turk.⁶ Each respondent rated 40 such vignettes taking approximately 10-12 minutes for each of the four surveys run as described in Table 2 and summarized in Table A1 in the Appendix. Common to all survey vignettes was a general overview about the type of information tracked by the website, varying between location, demographic, history of websites, and information only voluntarily provided. In addition, the website’s purpose – such as banking, photo sharing, search, travel – was varied. This provided a realistic common backdrop for all four factorial vignette surveys. See Table 3 for vignette factors and Table 4 includes the sample vignettes.

Table 3: Factorial Vignette Factors

Factor	Levels	Operationalized
Primary Use	TailorUse	tailor services for you
	DiscountUse	offer you discounts
	ImproveUse	provide a faster and more user-friendly website
	AdUse	place advertising targeted to you
Secondary Use	Friend2ndUse	The site sends advertising to friends and contacts
	Sell2ndUse	The site sell to tracking company who combines the data with your other activities
	Research2ndUse	The site may conduct research experiments using you and other users
	Internal2ndUse	The site removes your name from the data and uses the data to improve their service
Security	Null2ndUse	Null
	Hacker	An outsider then used a flaw in the website to download user records
	NiceHack	A researcher then found a flaw in the website to suggest a security fix
	Law	The information is stored and easily available to law enforcement as needed
	Null	Null

⁶ Turk has been used for consumer perceptions in marketing (Goldstein et al. 2014; Yang and Lynn 2014). In addition, a recent survey replicates (and extends) a Pew Research Study (Pew Research Center 2014a) privacy expectations around sensitive information on MTurk (Martin and Nissenbaum 2016).

Table 4: Vignette Factors Tested in Each Survey

Concept	Operationalized as (1 level shown)	Factorial Vignette Surveys			
		1	2	3	4
Primary Use (4 levels)	The <u>search</u> site uses the data to <u>tailor</u> <u>services for you</u>	X	X	X	X
Secondary Use (Null + 4 levels)	The site keeps the data to possibly conduct research experiments using you and other users.		X		X
Security Violation (Null + 3 levels)	An outsider then used a flaw in the website to download user records.			X	X

Respondent Controls in Each Survey

Before and after the vignettes, the respondents were asked several control questions. Respondents' age and gender were collected before the vignettes whereas the privacy, online knowledge and experience, and trust controls were asked after the vignettes to avoid priming the respondents. See Table A2 in the Appendix for the control variables included.

Rating Task

Consistent with the factorial vignette survey methodology, a single rating task remained the same for all vignettes (Jasso 2006a; Wallander 2009a). The focus of Surveys 1-4 is the highly particular consumer trust in a firm. Consumer trust, as the willingness to be vulnerable based on perceptions of the reliability and integrity of a firm (Garbarino and Johnson 1999; Mayer, Davis, and Schoorman 1995), is key for increasing purchase intentions (Lee and Turban 2001; Schlosser, White, and Lloyd 2006); trust encourages lower opportunism and increases customer loyalty (Grayson, Johnson, and Chen 2008). Importantly, actions that conform to the norms of the exchange relationship build trust and actions that violate norms of the exchange relationship detract from trust, since norms of exchange relationships form the guidelines of

appropriate behavior (Cropanzano and Mitchell 2005). Without trust, consumers are likely to disengage from the primary website tracking their behavior: the formation of trust is key for a consumer's "willingness to engage in an exchange relationship" at the level of vulnerability required online (Johnson and Selnes 2004, p. 4). This willingness to engage is the outcome of the experiment described below.

For each vignette, respondents were instructed: "Tell us how much you agree with the statement below. Using a sliding scale from 'strongly disagree' to 'strongly agree'. Respondents rated their agreement with the following prompt for each vignette: "I trust this website."⁷

Multilevel Analysis

The factorial vignette methodology creates a unique dataset with multiple judgments or ratings (40) for each respondent. The analysis then identifies the main factors that impact the respondent's trust in the website without directly asking the respondent, 'what is important to you when judging a website's practices and how important is it?' The resulting data set can be thought of in two levels: the vignette contextual factors and the respondent control variables. If I is the number of the respondents with level 2 individual variables and K is the number of vignettes answered with level 1 factor variables, the general equation is:

$$(1) Y_{ij} = \beta_0 + \sum \beta_k V_{jk} + \sum \gamma_h R_{hi} + u_i + e_j$$

where Y_{ij} is the rating of vignette k by respondent n , V_{jk} is the k^{th} factor of vignette j , R_{hi} is the h^{th} characteristic of respondent i , β_0 is a constant term, β_k and γ_h are regression coefficients for k

⁷ See also Rossiter (2002) on single item measures as well as Schumann, von Wangenheim, and Groene (2014) on the tension in marketing literature around single item measures. The factorial vignette survey methodology relies on a single rating task by design as the multiple vignette factors capture the complexity of the concept.

vignette factors and h respondent factors, u_i is a respondent-level residual (random effect), and e_j is a vignette-level residual.

SURVEY EXPERIMENT 1: PRIMARY USE OF INFORMATION AND COSUMER TRUST

Survey 1 tests if primary uses of information positively impact trust and serves as a baseline trust measurement for later comparison. The first experimental study was placed on Amazon Mechanical Turk (MTurk) where 393 participants rated 40 vignettes and control questions for a total of 15,720 vignettes. Respondents were paid \$2 per completed survey; participants were restricted to U.S. and approval rating over 90%.⁸

In addition to the baseline vignette described above with the context of the website and the type of information gathered, the vignettes in Survey 1 included the primary uses of information (e.g., tailor services, offer discounts, or place advertising). The scenarios presented in the vignettes looked like the following; the underlined portions are the contextual, primary use:

A general online search site silently collects the history of websites you visited.

The search site uses the data to tailor services for you and stores the data for 1 year.

The model conceptualizes the ratings as a function of the contextual factors described in the vignette (ΣV_k) and the characteristics of the respondent (ΣR_h) as explained in equation (1) above. Specifically, the equation for Survey 1 with primary use of information is:

⁸ Respondent fatigue was checked by controlling for later vignettes in the respondents' sequence (the sequence number of the vignette was captured and ranged from 1-40). While respondent fatigue was not a factor, a respondent learning curve has been important to check in previous vignette studies (Martin 2012); respondents appear to take 1-2 vignettes to acclimate to the format. The analysis was run minus the first 2 vignettes for each respondent and the results remained the same.

$$(2) \text{ Trust Judgment} = Y_{ij} = \beta_0 + \beta_1 \text{TailorUse} + \beta_2 \text{DiscountUse} + \beta_3 \text{ImproveUse} + \Sigma \gamma_h R_{hi} + u_i + e_j$$

The term β measures the effect of the consumer being exposed to the primary use of information in the vignette. For example, β_1 measures the important of using the information to tailor services to the consumer rather than the null (using information for advertising).

Table 5: Multilevel Regression Results for Survey Experiments

Multi-Level Regression Results of Rating Task on Vignette Factors								
Vignette Factors:	Survey 1		Survey 2		Survey 3		Survey 4	
	Primary Use		Primary + Second Use		Primary Use + Security		Primary + Second + Security	
	β	s.e.	β	s.e.	β	s.e.	β	s.e.
Primary Use								
TailorUse	8.48**	0.88	7.14**	0.94	4.79**	0.92	3.31**	0.95
DiscountUse	10.63**	0.88	6.06**	0.93	5.87**	0.92	4.37**	0.94
ImproveUse	14.03**	0.88	7.80**	0.93	8.67**	0.91	5.48**	0.94
(null = Ad Use)								
Marketing Secondary Use								
Friend2ndUse			-46.75**	1.05			-27.22**	1.05
Sell2ndUse			-48.77**	1.06			-30.85**	1.05
Research2ndUse			-18.63**	1.04			-11.32**	1.05
Internal2ndUse			9.24**	1.05			7.00**	1.05
(null = No 2ndUse)								
Security Violation								
Hacker					-47.88**	0.92	-36.83**	0.94
NiceHack					-18.05**	0.92	-9.75**	0.94
Law					-16.29**	0.92	-9.78**	0.95
(null = No Hack)								
Statistics								
DV	-8.47		-16.98		-18.43		-25.23	
SD	28.95		29.46		28.25		27.35	
ICC Null	28.8%		27.1%		26.9%		25.0%	
Respondent R2	0.695		0.744		0.711		0.742	
N (Users)	393		381		400		399	
N (Vignettes)	15720		15240		16000		15960	

** $p < 0.001$; * $p < 0.01$

To examine if the use of information to improve consumers' online experience will positively impact trust, the dependent variable was regressed on the vignette and respondent factors for Survey 1 as shown in Table 5. The results illustrate that the use of information to tailor services ($\beta = +8.48$, $p < 0.00$), offer discounts (+6.33), and improve the website (+14.03) positively impacts trust thereby supporting that consumers disclose information with an understanding of the beneficial, primary use of that information.

SURVEY EXPERIMENT 2: MARKETING SECONDARY USE AND CONSUMER TRUST

H1a and H1b offer two alternatives to the privacy norms within the marketing exchange relationship online. To test whether secondary uses of information for tracking and targeting users is outside the privacy norms of the exchange and a violation of trust, Survey 2 included the baseline primary uses of information (Survey 1) plus the secondary use of information, which varied by changing the use of information as well as including a secondary actor as shown in Figure 2. H1a and H1b examine whether the use of information outside the immediate context or by actors outside the exchange are violations of the privacy norms of the exchange relationship. The secondary use of information for marketing was operationalized as selling to a data aggregator, sending advertising to friends and contacts, conducting research, and improving the website's service in order to include both alternative uses of information as well as alternative actors. Figure 2 illustrates the vignette factors by use and actor.

Figure 2: Vignette Factors By Contextual Use and Primary Actor (coefficients of factors included). Red signifies negative impact on consumer trust; Blue signifies positive impact on consumer trust.

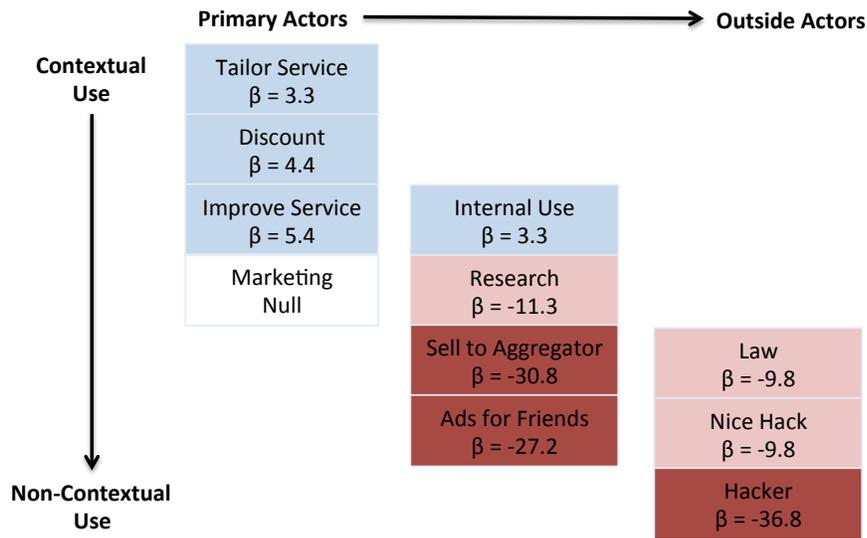
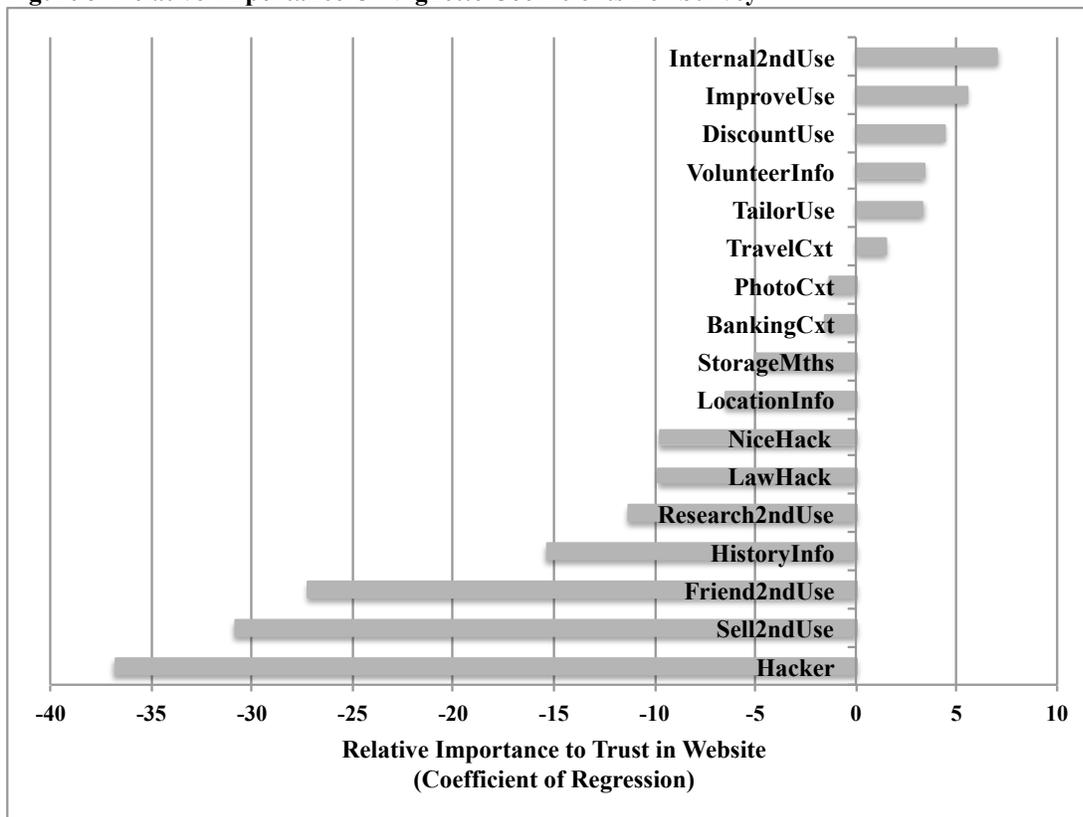


Figure 3 Relative Importance Of Vignette Coefficients For Survey 4



The scenarios presented in the vignettes looked like the following for survey experiment 2 (bolded is new to this survey but was not bolded in the actual survey). Similar to Survey 1, the underlined portion changed based on the levels in Table 5.

A general online search site silently collects the history of websites you visited.

The search site uses the data to tailor services for you and stores the data for 1 year.

The site keeps the data to possibly conduct research experiments using you and other users.

In Survey 2, the secondary use of information is added to the vignette in order to compare possible to the importance of primary use of information. Equation (2) is appended to include:

- $\text{Marketing 2}^{\text{nd}} \text{Use} = + \beta_{11}\text{Friend2ndUse} + \beta_{12}\text{Sell2ndUse} + \beta_{13}\text{Reserch2ndUse} + \beta_{14}\text{Internal2ndUse}$

The dependent variable – consumer trust in the website – was regressed on the vignette and respondent factors for Survey 2. The results are in Table 5. The results show that two secondary and non-contextual uses of information, selling information to a data aggregator ($\beta = -48.77, p < 0.00$) and using information to target contacts and friends ($\beta = -46.75, p < 0.00$), negatively impact trust of the firm even when the scenario contains beneficial uses of information and general context of the use of information. These findings do not support H1a that the use of information online by additional actors and future uses will be judged to be within the consumers' marketing exchange relationship online and, therefore, not impact consumer trust in the website.

Instead, H1b – that the use of information online by additional actors and future uses will be judged to be outside the consumers' marketing exchange relationship online and, therefore, negatively impact consumer trust in the website – does find support with these findings. The results suggest that consumers consider the secondary use of information to be outside the privacy norms of the marketing exchange relationship. Instead, privacy norms of the marketing exchange relationship online includes whether the information is used in a contextually appropriate manner

H2 states that regardless of the norm of privacy (H1a versus H1b), consumers perceive the benefits of tracking to outweigh any perceived harms and risks. To test H2, we examine the relative importance of primary uses compared to the secondary use of information. We would expect that the benefits of the primary use of information to outweigh and be significantly larger than any potential costs associated with secondary uses.

The results show that the two secondary uses of information – changing the actor using the information (selling to a data aggregator) and changing the use of information (to target friends – have statistically the same impact on consumer trust ($\chi^2 = 1.38, p = 0.24$) yet are significantly greater impact on trust in the firm than the primary uses of information. In fact, the addition of the secondary use of information to the vignettes drives down the average trust rating of the vignettes to -16.98 in Survey 2 compared to -8.47 for Survey 1 when only the primary use of information was included ($t = 13.53, p = 0.00$). The results support that the secondary use of information – to include selling to a data aggregator, using information to target friends, and conducting research on the consumer – negatively impacts consumer trust in a website and outweighs the positive impact of the primary use of information by driving down the overall consumer trust in the website. The findings do not support H2 that consumers positive perceive

a tradeoff between the costs and risks of secondary uses of information as being outweighed by the benefits of sharing information.⁹

SURVEY EXPERIMENT 3-4: IMPORTANCE OF PRIVACY V. SECURITY

To further identify the relative importance of respecting privacy norms of the marketing exchange relationship, Surveys 3 and 4 compare the impact of violating privacy norms and security violations on consumer trust. As noted in H3, a security violation will do more damage to trust in a website than the secondary use of information for marketing since security violations are well outside any exchange agreement with consumers (Dunfee, Smith, and Ross Jr 1999; Schumann, von Wangenheim, and Groene 2014). Security violations are outsiders (e.g., hackers) who cause harm by damaging a system or accessing, disclosing, and misusing consumer data (Belanger, Hiller, and Smith 2002b; Flavián and Guinalíu 2006; Miyazaki and Fernandez 2000).

Survey 3 included the baseline (Survey 1) plus security violations defined as an outside intruder accessing the websites' information about the consumer. To isolate the importance of (a) an outsider with (b) the intent to do harm, three security violations were varied: a researcher identifying as security flaw to help the website (NiceHack), an outsider then using a flaw in the website to download user records (Hacker), and law enforcement having access to the data

⁹ In fact, the average trust rating for respondents was -8.47 when only beneficial primary uses were included as shown in Table 5, suggesting that, on average, respondents distrust websites even for their primary use of information. However, the average trust rating for websites in the vignettes is more than the average institutional trust in websites suggesting respondents trust specific websites more when the details of the primary use of information is described (institutional trust-in-websites = -11.77); in addition, the average trust rating when the data in the vignette is stored for only the immediate session is positive (+20.87). The results support that the primary use of information positively impacts trust in the website, and that the average consumer trust in a website is positive when storage of information is minimized.

(Law). All are outsiders to the firms-consumer relationship with different intentions – see also Figure 2.

The scenarios presented in the vignettes looked like the following – bolded is new to this survey with the underlined portion varying based on the levels in Table 4.

A general online search site silently collects the history of websites you visited.
The search site uses the data to tailor services for you and stores the data for 1 year.
A researcher then found a flaw in the website to suggest a security fix.

In Survey 3, Equation (2) is appended to include:

Possible Security Violations: $+ \beta_{15}\text{Hacker} + \beta_{16}\text{NiceHacker} + \beta_{17}\text{Law}$

H3 states that regardless of the norm of privacy (H1a versus H1b), security violations will be significant larger threats to the norms of the marketing exchange relationship online and, therefore, have a significantly larger negative impact on consumer trust in the website compared to a violation of the privacy norm. We would expect that the importance of violating privacy norms through the secondary use of information will be significantly less than the importance of security violations by outside parties. To test H3, the dependent variable – consumer trust in the website – was regressed on the vignette and respondent factors for Survey 3. The results are in Table 5 and Figures 2 and 3. Not surprisingly, security violations, in the form of an outsider gaining access to consumer information, negatively impacted trust in the website and outweighed the positive impact of the primary use of information.

However, and counter to H3, the impact on trust of a hacker accessing the data ($\beta = -47.88$, $p < 0.00$) is the same as when a website sells information to a data aggregator ($\beta = -46.75$; $\chi^2 = 0.04$, $p = .85$) or uses information to target friends ($\beta = -48.77$; $\chi^2 = 0.52$, $p = 0.47$) in Survey 2 thus not supporting H3. In other words, consumers appear to equate secondary use of

information for marketing, such as a website selling information to a data aggregator or using the information to retarget friends, to security violations in terms of (dis)trusting the website. The relative importance of secondary use of information to consumer trust (Survey 2) is statistically equal to the outsider taking the data (in Survey 3).

To further test this surprising finding, Survey 4 was run to have the respondents directly compare the secondary use of information and security violations in the same vignette. Survey 4 included the Survey 2 plus security factors.

The results are in Table 5 and Figures 2 and 3. Here the negative impact of the security violations ($\beta_{\text{hacker}} = -36.83$, $p < 0.00$) has a slightly greater impact on consumer trust than secondary use of information such as selling information to a data aggregator ($\beta_{\text{sell}} = -30.85$, $p < 0.00$) or to use for retargeting friends ($\beta_{\text{friend}} = -27.22$, $p < 0.00$) thus partially supporting H3.

In addition, across both Survey 3 and Survey 4, a benevolent hacker seeking to identify a security flaw ($\beta = -9.75$, $p < 0.00$) is considered statistically the same impact on trust as law enforcement gaining access to the data ($\beta = -9.78$; $\chi^2 = 0.06$, $p = .80$). These results are illustrated in Figure 2 with shades of red depicting types of behavior outside the privacy norms of the marketing exchange relationship and shades of blue depicting types of behavior within the privacy norms of the marketing exchange relationship.

When tested separately, a security violation of a hacker accessing consumer information diminishes trust in a website in a manner similar to marketing secondary use of information. However, when tested simultaneously in Survey 4, the impact of a security violation of an outsider gaining access to the consumer information is slightly more negative than the secondary use of information for marketing on consumer trust.

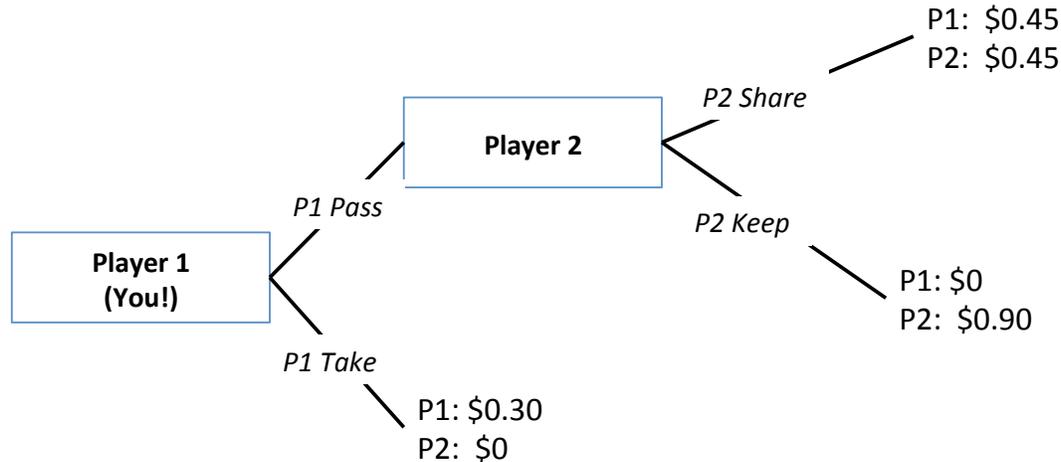
EXPERIMENT: PRIVACY NORMS AND WILLINGNESS TO ENGAGE

In order to further test the finding that the norms of consumer exchange online do not include pervasive tracking and secondary uses for marketing, we sought to measure the impact of tracking and behaviorally targeted advertising on the trust *behavior* or a consumer's willingness to engage. A recurring limitation in capturing only the trust judgment of respondents or trust intent is having no direct measure of their willingness to become vulnerable (McKnight, Choudhury, and Kacmar 2002). One tool utilized in behavioral economics and organizational behavior research is the "Trust Game" to measure trust in a trustee (Anderhub, Engelmann, and Güth 2002; Berg, Dickhaut, and McCabe 1995). The trust game has been used to measure both trustworthy factors of partners as well as general contextual factors that impact trusting behavior (Malhotra 2004; Malhotra and Murnighan 2002). In some surveys, the trust game (or investment game) is played between two people in a lab. Here, we are interested in an individual's trust in a website so the respondent is assigned to be one player (Player 1) and plays the game online with a 'website' (Player 2) designed with particular attributes. Player 1 must decide to become vulnerable to Player 2 by passing the initial amount of money and trusting Player 2 will share the proceeds back.

Participants were told they would play four rounds with the same partner, and each participant made four separate decisions. Each round of the scenario occurred in two stages as shown in Figure 4. For example, Player 1 was endowed with \$0.30 at the start of each round. Player 1 player made the first decision and could pass \$0.30 or take \$0.30. If Player 1 chose "Take", they earned \$0.30, Player 2 earned \$0, and the round ended. If Player 1 chose "Pass" (Trust), the amount of money grew to \$0.90, and Player 2 decided whether or not to share the

\$0.90 with Player 1. In each round, both Player 1 indicated their choice. Participants learned each round what Player 2 decided and could take Player 2's behavior into account in the next round.

Figure 4: Diagram of Trust Game Experiment to Measure Propensity to Trust as Shown to Respondents



The respondent was assigned to be Player 1 and would decide whether or not to trust Player 2 by passing the endowed/initial amount. The outcome was binary (0/1) as the respondent could only pass or not pass to Player 2. The experiment measures actual trust behavior rather than a normative judgment or trust intent. By changing the attributes of the programmed website who is Player 2 (e.g., if Player 2 used privacy preserving ads versus pervasive tracking), we measured the trustworthiness of Player 2 as dependent on the contextual choices Player 2 made in regards to consumer tracking.¹⁰ After each of the four rounds, we also asked participants, “How much do you trust your partner?” (1: Completely Trust, 7: Do Not Trust at All).

Standard controls from the previous surveys were used.

¹⁰ A meta analysis of the Trust Game in economics found important differences in trusting an individual in a lab versus trusting online with a programmed agent such as a website (Johnson and Mislin 2011). Since the unit of interest in the consumers' willingness to engage with a website, including Player 2 as a website most clearly replicated the actual phenomenon of interest.

Sample

American participants were recruited from Amazon Mechanical Turk (46% female and median age range of 25-34 years old). Each participant received \$1.00 for taking the survey regardless of the outcome of the experimental game. In addition, respondents would receive a bonus of up to \$0.50 based on the results of the trust game and their overall ‘diligence’ in taking the survey.

The respondents received the following instructions:

In this part of the experiment, you will make several decisions in an interactive scenario that allows two players to earn money – Player 1 and Player 2. You are Player 1.

First, you will learn the rules of the scenario, and then you will learn the attributes of Player 2.

The experiment consists of 4 rounds in total, and each player will make 4 separate decisions.

Each round of the scenario occurs in two stages: In the first stage, you (Player 1) choose PASS (Invest) or NO PASS (Take).

1. If you choose NO PASS, the round ends and you earn \$0.30 .
2. If you choose PASS, then the money is tripled and Player 2 has \$0.90 to either share or keep.
 - If Player 2 chooses SHARE, then you both split the \$0.90 and each earn \$0.45.
 - If Player 2 chooses KEEP, Player 2 keeps the \$0.90 and you earn \$0.00

Bonus Payment

Within 24 hours after the experiment, we will choose one round from this scenario and you will receive a bonus payment based on your decision and the decision of Player 2. This payment is in addition to your \$1.00 payment for completing the HIT. You can also earn a bonus for paying attention throughout.

Thank you for participating!

After the control questions, respondents were told “You have been randomly assigned one of three possible versions of Player 2. For you, Player 2 is a website where the designer of the website wrote a program to respond to each of your decisions. For full disclosure: ...” and then

given one of three conditions:

- A. Ad Network (N = 202): *In the course of his other work, Player 2 supports his website by selling access to his users' behavioral information using an online advertising network that collects user behavior (browsing, purchases, searches, etc) to offer highly personalized ads based on consumers' online history. Data brokers can then combine the consumer information from other sources online and offline for later use.*
- B. Privacy Preserving (N = 227): *In the course of his other work, Player 2 supports his website by offering ads without tracking the user specifically. The designer (Player 2) has decided to not disclose any personal information such as a user identifier or behavior to data brokers or ad networks.*
- C. Security Violation (N = 227): *In the course of his other work, Player 2 was unfortunately recently hacked and had user data downloaded by a third party. It is not clear who attacked the website.*

Table 6: Percent of Respondents who pass the endowed amount to Player 2 each round by condition

Percent Who Pass					
	N	R1	R2	R3	R4
Generic *	200	72%	73%	82%	76%
PrivacyPreserving	227	73%	78%	82%	81%
AdNetwork	202	64%	74%	73%	78%
Hack	227	64%	70%	77%	78%

* A separate study was run without any mention of the privacy or security practices of Player 2. The results of the 'generic' Player 2 serve as a baseline here.

Results

H4 states that practices outside the privacy norms of the marketing exchange will negatively impact consumers' willingness to engage with a partner. To test H4, the percent of respondents who passed to player 2 (trusted player 2 or was willing to engage with Player 2) was calculated for each round and by each type of Player 2 (Privacy Preserving, Ad Network, Security Violation). The results are in Table 6.

Consistent with H4, partners who were described as using practices within the privacy norms of the marketing exchange relationship tested above (Privacy Preserving) were trusted more frequently (73%) than partners who utilized pervasive tracking techniques for marketing (64%) ($t = -1.96, p = 0.02$). Repeated trustworthy behavior by Player 2, by sharing the windfall of the tripled endowment across four rounds, diminished any difference in trust for privacy preserving and pervasive tracking partners as shown in Table 6.

In order to examine how respondents with high and low institutional trust differ in the trust game experiment, High Trust was defined as respondent who answered that they moderately or completely trust websites (a 4 or 5 in the control) and Low Trust was defined as respondent who stated they only slightly or not at all trusted websites generally. This control question was asked before the experiment began. See Table 7.

Table 7: Respondent Institutional Trust in Websites

	Trust Sites	Frequency	Percent	Cumulative
Low Trust	Not at All	24	3.66	3.66
	Slightly	159	24.24	27.9
Moderate Trust	Somewhat	306	46.65	74.54
High Trust	Moderately	162	24.7	99.24
	Completely	5	0.76	100
	Total	656	100	

Figures 5 and 6 show no difference in initial trust or a willingness to engage between Player 2 conditions (privacy preserving versus ad network) for *high trust respondents*. In addition, respondents with low institutional trust in website (28% of the sample) were able to rebuild their trust in the partner for privacy preserving partners (the dashed grey line in Figure 5) but not for partners utilizing an ad network with pervasive tracking for marketing.

Perhaps most concerning for publishing websites, respondents with moderate institutional trust (47% of the sample) were the most impacted by Player 2’s decision to use an ad network and breach the norms of the marketing exchange. Figure 6 shows 60% of moderate-trusting respondents willing to engage with Player 2 using an ad network versus 75% willing to engage in round 1 for privacy preserving Player 2 in Figure 5. Moderately trusting respondents are willing to rebuild trust if shown trustworthy behavior as evidenced by their 80% willing to engage in round 4 in Figure 5 if required to work with the website as in this experiment.

The decision of a partner, such as Player 2 in this experiment, to breach privacy norms by using an ad network impacts an individuals’ willingness to engage. Put another way, breaching the privacy norms of the marketing exchange by using an ad network leads more consumers to chose a competitor or walk away from a particular website particularly for individuals with moderate and low institutional trust.

Figure 5: Percent of Respondents who Trust for Privacy Preserving Player 2 by Respondent Trust

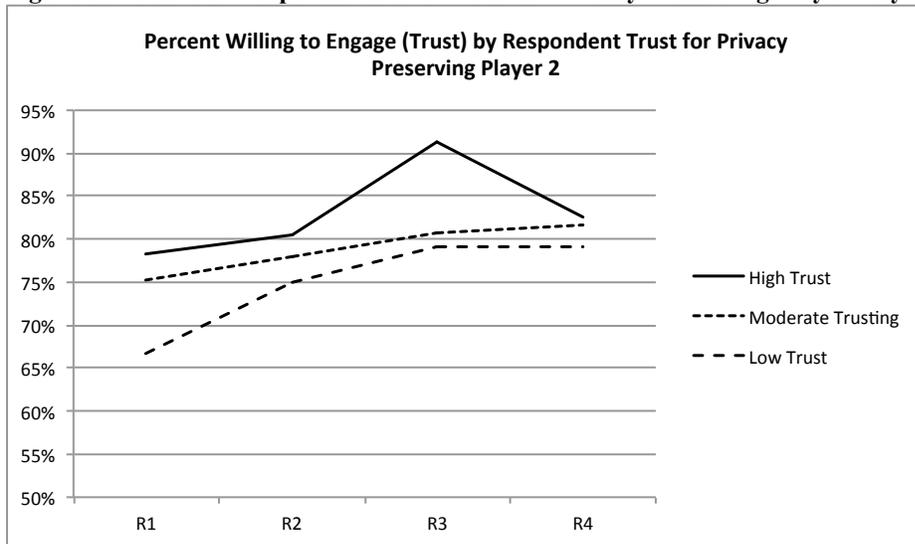
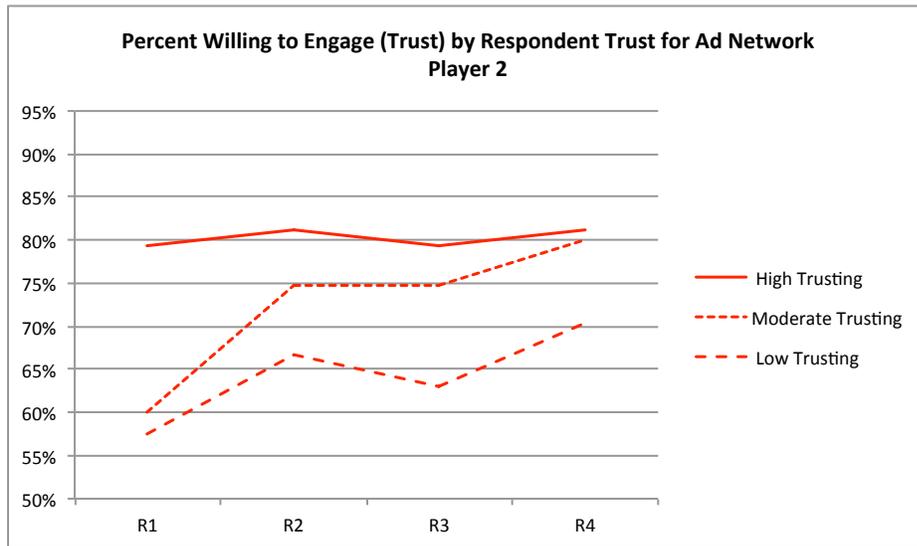


Figure 6: Percent of Respondents who Trust for Ad Network Player 2 by Respondent Trust

DISCUSSION AND CONCLUSION

The results demonstrate that the privacy approach implicit in the norms of consumer marketing exchange online are consistent with privacy as the context appropriate use or flow consistent with previously theorized definitions of privacy (Martin 2015b; Nissenbaum 2010): consumers judged the contextual, primary use of information as within the exchange but the secondary, non-contextual use of information to be outside the exchange and a violation of trust. Further, and consistent with privacy as the contextually appropriate use of information, the secondary uses of information – selling consumer information to data aggregators and targeting friends – are considered on par with a security violation of an outsider (i.e., a hacker) stealing information from a website.

In addition, the results demonstrate that respecting privacy norms is important to consumers' economic behavior. The trust game experiment shows respondents are less willing to engage with a partner who violated privacy norms of the exchange relationship and utilized

pervasive tracking. Consistent with previous research (Martin, Borah, and Palmatier 2016), respondents with low institutional trust in websites were able to rebuild their trust with partners respecting privacy norms but not for partners breaching privacy norms of the exchange relationship by utilizing pervasive tracking for marketing. Importantly, breaching the privacy norms of the marketing exchange by using an ad network leads more consumers to chose a competitor or walk away from a website particularly for individuals with moderate and low institutional trust.

These results contradict the view that consumers give up privacy when engaging with a website and suggest that tracking for online marketing is considered a violation of consumer trust for websites. The study has managerial and theoretical implications.

Managerial Implications

If consumers perceive privacy violations, such as selling information to a data aggregator, on par with a security violation, such as a hacker accessing personally identifiable data, then marketers online could face a consumer backlash once the practices are known. Identifying product harm and consumer vulnerability is key to the ethical evaluation of marketing strategies (Jones and Middleton 2007). Yet, previous scholarship shows consumers do not know about many information practices online (Martin 2015a). The results here suggest that the ethical evaluation of marketing strategies online may be still to come as consumers become more knowledgeable about information practices.

This study suggests that not all privacy and security violations are created equal and more work should be done to identify the key drivers of consumer distrust to focus efforts on ensuring such practices are modified to retain the consumers trust. For example, if secondary uses of

information – such as selling to a data aggregator or using information to target friends – are needed by firms, more work must be done to render these actions less risky for consumers. Managers seeking to cultivate consumer trust may seek alternatives such as limiting the use of privacy invasive tactics or finding technological solutions to limit personally identifiable information.

Marketers could limit the use of personal information shared and used for marketing as recent research has illustrated the limits in effectiveness of personalized marketing tactics online (Lambrecht and Tucker 2013). Contextual ads have been found to be a viable and attractive alternative (Goldfarb and C. Tucker 2011b); similarly, dynamic retargeting, which requires highly personal information reused from previous online sessions, is found to be useful only when consumers are narrowing in on a purchase (Goldfarb and C. E. Tucker 2011a). Future work could continue to find the limits of invasive marketing tactics or alternatives that are viable while maintaining consumer trust in a firm. Advertising partners who offer technological solutions, such as using differential privacy and pseudo-anonymous tracking, could offer effective advertising without the privacy invasive tactics.

The perception of vulnerability from security violations has become the focus of public policy. Firms' consumer information security practices are increasingly the subject of government scrutiny through the FTC as well as through regulations of specific industries such as FINRA and HIPPA. The U.S. Congress proposed the Data Security Act of 2015 to set minimum standards for the security of consumer data from outside access. And the SEC has elevated the issue of cybersecurity to the level of the board of directors of public companies to maintain the integrity of the markets (Aguilar 2014). If secondary uses of information are seen

as akin to security violation, a renewed effort to regulate secondary use of information could mirror the efforts around security.

This study has implications for the relationship between firms and marketers. Previous research has shown how the interests between consumer facing firms (publishers) and online marketing can be re-aligned. The data driven marketing firms, such as ad networks, data aggregators, and data brokers, have benefited with better click through rates when the primary website includes better privacy controls (Tucker 2014). Where Tucker's (2014) research illustrates why data driven marketing firms should care about the privacy controls of the primary website, this research suggests that primary websites should similarly care about how information is being tracked and used by marketers. This study illustrated how websites are blamed for the tracking and secondary use of information by marketers: consumer trust in a website was negatively impacted by dynamically targeting contacts and friends and by selling information to a data aggregator. The interests of the larger online marketing ecosystem – to include data aggregators, data brokers, ad networks – to gather aggregate and selling personally identifiable information may not be aligned with the interests of firms to maintain consumer trust.

Theoretical Implications

Exchange relationships. This research contributes to scholarship on exchange relationships in marketing. In particular, several theories of relationship marketing propose that customers vary in their relationships with a firm on a continuum from transactional to highly relational bonds (Garbarino and Johnson 1999); for high relational customers, trust and commitment are important for loyalty (Garbarino and Johnson 1999). Yet, recent work has

suggested that consumers online both choose and are forced out of transaction exchanges and into relationship exchanges. Consumers are not given the option to make anonymous, discrete transactions and are forced into a relationship exchange – or “cooperative relationship based on trust” (Hoffman, Novak, and M. A. Peralta 1999, p. 82). In other word, firms may have pushed consumers into relationship exchange with greater information risk and vulnerability and where trust is more necessary. These results reinforce why a reciprocity argument may be more effective than a more transactional approach in developing consumer trust around privacy (Schumann, von Wangenheim, and Groene 2014) as well as framing the consumer-firm transaction as a relationship rather than a mere economic exchange (Hoffman, Novak, and Li 2015).

Public policy. The implications for public policy are twofold: both the substance and scope of regulations could be impacted by these findings. First, attempts to regulate privacy expectations online have focused on notification and user choice. These results could be viewed as identifying minimums for consumer trust for notification concerning privacy standards. Minimum standards for web practices have been called for in research on notices (Marotta-Wurgler 2014), and the findings here identify web practice of particular concern to consumers. Further, the findings illustrate the degree of consumer *agreement* around privacy violations as impact consumer trust furthering supporting the push for privacy minimums for notices.

Second, the study illustrates privacy violations as impacting consumer trust, which may broaden the purview of regulators currently focused security. More broadly, the results identify the importance of privacy violations to consumer trust on par with security violations. These findings could provide evidence for regulations concerned with consumer trust to focus on privacy if firms to not take responsibility themselves through private ordering. This is

problematic as previous work suggests that blanket regulations such as Do Not Track limits the use of data by firms and reduces ad effectiveness (Beales 2010; Goldfarb and C. E. Tucker 2011a) suggesting firms attempting to identify reasonable limits about broad user tracking would be preferable to regulations. Given the limited effectiveness of notices (Martin 2014; Barocas and Nissenbaum 2009) and consumer choice (John, Acquisti, and Loewenstein 2011), firms appear best positioned to navigate consumer minimums for privacy online.

Consumer vulnerability. This study shows how marketing practices could make consumers *more* vulnerable by increasing perceived information risk. As has been noted previously, marketing both reduces and contributes to consumer vulnerability (Shultz and Holbrook 2009). Scholarship on consumer vulnerability focuses on consumers “who are more susceptible to economic, physical, or psychological harm in, or as a result of, economic transactions” (Dunfee, Smith, and Ross Jr 1999, p. 4). While much work has been placed on marketing to currently vulnerable consumers, this study suggests specific marketing tactics, such as broad user tracking and reusing information, contribute to creating vulnerable consumers. The collection and use of personally identifiable information increases information risk and perceived consumer vulnerability. In fact, certain marketing tactics – such as storing and distributing personally identifiable information – could leave consumers particularly vulnerable when, as noted by Jones and Middleton (2007), individuals do not know what is good for them and do not have the resources (knowledge) to fix the problem.

Limitations and Future Research

Measuring consumers’ valuation of privacy in field experiments can be problematic (Acquisti, John, and Loewenstein 2013). Field studies have limitations, as consumer behavior

does not necessarily take into consideration the actual disclosure, storage, sharing, and aggregation of their information.¹¹ Consumers online face a high degree of information asymmetry around the information practices of firms (Martin 2013). Effective communications of online marketing practices is limited as our current notification approach is time intensive for consumers (McDonald and Cranor 2008), often misunderstood (Leon et al. 2012), and acts as a blank slate for consumers' desired privacy practices (Martin 2015a). Consumer tracking has remained obscured from consumers (Brunton and Nissenbaum 2011; Nissenbaum and Brunton 2015).¹²

While this study identifies how consumer judgments and reactions to privacy norms of the marketing exchange when the firm's practices are known, more work is needed on how to communicate the information practices to consumers to maintain a willingness to disclose information. Research has found consumer willingness to disclose depends on the exchange order and whether the transaction is contingent or not on the disclosure of information (White, Novak, and Hoffman 2014). When engaging with a website is contingent upon consumers disclosing information, the order in which the request for information is made is not significant to a willingness to disclose. However, if consumers make disclosure optional, by using anti-tracking software or blockers on their web browser, how consumers are asked for information will impact their willingness to disclose (White, Novak, and Hoffman 2014). Such research will be critical as users continue to gain knowledge about the pervasive tracking and are offered products to make tracking optional (Nissenbaum and Brunton 2015).

¹¹ Work by Tucker (Goldfarb and C. Tucker 2011b; Goldfarb and C. E. Tucker 2011a; b; Tucker 2012, 2014) is a notable exception to the usual limitations; Tucker shows how important measurements such as purchase intent and click-through rates are impacted by regulations or firm privacy controls without making any assumptions as how 'informed' the consumer is of privacy practices.

¹² In fact, new tracking technologies work around consumer tracking identification (Ayenson et al. 2011; Soltani et al. 2010) requiring more sophisticated research to even be able to identify the 81,000 third-party trackers following consumers online (Englehardt and Narayanan 2016).

This study did not identify how uses of information and security impact trust given the trustworthy factors of ability, benevolence, and integrity (Mayer, Davis, and Schoorman 1995). More work should be done to identify if information practices impact the integrity of the firm or the ability of the firm. Previous work identifies benevolence and integrity as important consequences of information practices when the concepts are operationalized as privacy and security statements (Schlosser, White, and Lloyd 2006). However, identifying whether and how marketing information practices impact trust factors of ability and integrity would provide guidance to firms on how to repair consumer distrust.

Conclusion

Marketing online has become increasingly dynamic and personal necessitating consumers to take on greater information risk and, therefore, making privacy and security key for consumer trust online. This paper illustrates the potential cost to consumer facing firms to breaking the privacy norms of the marketing exchange. The interests of the larger, hidden online marketing ecosystem – to include data aggregators, data brokers, ad networks – to gather, aggregate, and sell personally identifiable information may not align with the interests of firms to develop the consumer relationship and maintain consumer trust.

REFERENCES

- Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein (2015), "Privacy and human behavior in the age of information," *Science*, 347 (6221), 509–14.
- , Leslie K John, and George Loewenstein (2012), "The impact of relative standards on the propensity to disclose," *Journal of Marketing Research*, 49 (2), 160–74.
- , ———, and ——— (2013), "What is privacy worth?," *The Journal of Legal Studies*, 42 (2), 249–74.
- Aguilar, Luis (2014), "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," New York Stock Exchange.
- Anderhub, Vital, Dirk Engelmann, and Werner Güth (2002), "An experimental study of the repeated trust game with incomplete information," *Journal of Economic Behavior & Organization*, 48 (2), 197–216.
- Ayenson, Mika, Dietrich J Wambach, Ashkan Soltani, Nathan Good, and Chris J Hoofnagle (2011), "Flash cookies and privacy II: Now with HTML5 and ETag respawning," *Social Science Research Network*.
- Banerjee, Syagnik Sy and Ruby Roy Dholakia (2008), "Mobile advertising: does location based advertising work?," *International Journal of Mobile Marketing*.
- Barocas, Solon and Helen Nissenbaum (2009), "On notice: The trouble with Notice and Consent," 12–13.
- Bart, Yakov, Venkatesh Shankar, Fareena Sultan, and Glen L Urban (2005), "Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study," *Journal of Marketing*, 69 (4), 133–52.
- Beales, Howard (2010), "The value of behavioral targeting," *Network Advertising Initiative*.
- and Jeffrey A Eisenach (2014), "An Empirical Analysis of the Value of Information Sharing in the Market for Online Content," *Available at SSRN 2421405*.
- Belanger, France, Janine S Hiller, and Wanda J Smith (2002a), "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The Journal of Strategic Information Systems*, 11 (3), 245–70.
- , ———, and ——— (2002b), "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes," *The Journal of Strategic Information Systems*, 11 (3), 245–70.
- Berg, Joyce, John Dickhaut, and Kevin McCabe (1995), "Trust, reciprocity, and social history," *Games and economic behavior*, 10 (1), 122–42.
- Brunton, Finn and Helen Nissenbaum (2011), "Vernacular resistance to data collection and analysis: A political theory of obfuscation," *First Monday*, 16 (5).
- Calo, M Ryan (2011), "Boundaries of Privacy Harm, The," *Ind. LJ*, 86, 1131.
- Chellappa, Ramnath K and Raymond G Sin (2005), "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information Technology and Management*, 6 (2-3), 181–202.
- Cheung, Christy MK and Matthew KO Lee (2006), "Understanding consumer trust in Internet shopping: A multidisciplinary approach," *Journal of the American Society for Information Science and Technology*, 57 (4), 479–92.
- Crawford, Kate (2013), "The Hidden Biases in Big Data," *Harvard Business Review*.
- and Jason Schultz (2014), "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms," *Boston College Law Review*, 55 (1).
- Cropanzano, Russell and Marie S Mitchell (2005), "Social exchange theory: An interdisciplinary review," *Journal of management*, 31 (6), 874–900.
- Culnan, Mary J. and Robert J. Bies (2003), "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues*, 59 (2), 323–42.

- Dinev, Tamara and Paul Hart (2006), "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, 17 (1), 61–80.
- Dunfee, Thomas W, N Craig Smith, and William T Ross Jr (1999), "Social contracts and marketing ethics," *The Journal of Marketing*, 14–32.
- Englehardt, Steven and Arvind Narayanan (2016), "Online tracking: A 1-million-site measurement and analysis."
- Federal Trade Commission (2014), "Data Brokers: A call for transparency and accountability," FTC.
- Flavián, Carlos and Miguel Guinaliú (2006), "Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site," *Industrial Management & Data Systems*, 106 (5), 601–20.
- Gabisch, Jason Aaron and George R Milne (2014), "The impact of compensation on information ownership and privacy control," *Journal of Consumer Marketing*, 31 (1), 13–26.
- Ganong, Lawrence H. and Marilyn Coleman (2006), "Multiple Segment Factorial Vignette Designs," *Journal of Marriage and Family*, 68 (2), 455–68.
- Garbarino, Ellen and Mark S Johnson (1999), "The different roles of satisfaction, trust, and commitment in customer relationships," *the Journal of Marketing*, 70–87.
- Goldfarb, Avi and Catherine Tucker (2011a), "Search engine advertising: Channel substitution when pricing ads to context," *Management Science*, 57 (3), 458–70.
- and ——— (2011b), "Online display advertising: Targeting and obtrusiveness," *Marketing Science*, 30 (3), 389–404.
- and Catherine E Tucker (2011a), "Privacy regulation and online advertising," *Management Science*, 57 (1), 57–71.
- and ——— (2011b), "Online advertising, behavioral targeting, and privacy," *Communications of the ACM*, 54 (5), 25–27.
- Goldstein, Daniel G, Siddharth Suri, R Preston McAfee, Matthew Ekstrand-Abueg, and Fernando Diaz (2014), "The economic and cognitive costs of annoying display advertisements," *Journal of Marketing Research*, 51 (6), 742–52.
- Grayson, Kent, Devon Johnson, and Der-Fa Robert Chen (2008), "Is firm trust essential in a trusted environment? How trust in the business context influences customers," *Journal of Marketing Research*, 45 (2), 241–56.
- Grossklags, Jens and Alessandro Acquisti (2007), "When 25 Cents is Too Much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information."
- Hill, Ronald Paul and Kelly D Martin (2014), "Broadening the paradigm of marketing as exchange: a public policy and marketing perspective," *Journal of Public Policy & Marketing*, 33 (1), 17–33.
- Hoffman, Donna L, Thomas P Novak, and Yuanrui Li (2015), "Online Consumer Behavior," *The International Encyclopedia of Digital Communication and Society*.
- , ———, and Marcos Peralta (1999), "Building consumer trust online," *Communications of the ACM*, 42 (4), 80–85.
- , ———, and Marcos A Peralta (1999), "Information privacy in the marketplace: Implications for the commercial uses of anonymity on the Web," *The Information Society*, 15 (2), 129–39.
- Hui, Kai-Lung, Hock Hai Teo, and Sang-Yong Tom Lee (2007), "The value of privacy assurance: an exploratory field experiment," *Mis Quarterly*, 19–33.
- Iyer, Ganesh, David Soberman, and J Miguel Villas-Boas (2005), "The targeting of advertising," *Marketing Science*, 24 (3), 461–76.
- Jasso, Guillermina (2006a), "Factorial survey methods for studying beliefs and judgments," *Sociological Methods & Research*, 34 (3), 334–423.
- (2006b), "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods & Research*, 34 (3), 334–423.
- John, Leslie K, Alessandro Acquisti, and George Loewenstein (2011), "Strangers on a plane: context-dependent willingness to divulge sensitive information," *Journal of Consumer Research*, 37 (5), 858–73.

- Johnson, Michael D and Fred Selnes (2004), "Customer portfolio management: Toward a dynamic theory of exchange relationships," *Journal of Marketing*, 68 (2), 1–17.
- Johnson, Noel D and Alexandra A Mislin (2011), "Trust games: A meta-analysis," *Journal of Economic Psychology*, 32 (5), 865–89.
- Jones, Jeri Lynn and Karen L Middleton (2007), "Ethical decision-making by consumers: The roles of product harm and consumer vulnerability," *Journal of Business Ethics*, 70 (3), 247–64.
- Kim, Dan (2005), "Cognition-Based Versus Affect-Based Trust Determinants in E-Commerce: Cross-Cultural Comparison Study," *ICIS 2005 Proceedings*, 59.
- Kim, Dan J, Donald L Ferrin, and H Raghav Rao (2008), "A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents," *Decision support systems*, 44 (2), 544–64.
- Lambrecht, Anja and Catherine Tucker (2013), "When does retargeting work? Information specificity in online advertising," *Journal of Marketing Research*, 50 (5), 561–76.
- Lee, Matthew KO and Efraim Turban (2001), "A trust model for consumer internet shopping," *International Journal of electronic commerce*, 6 (1), 75–91.
- Leon, Pedro Giovanni, Justin Cranshaw, Lorrie Faith Cranor, Jim Graves, Manoj Hastak, Blase Ur, and Guzi Xu (2012), "What do online behavioral advertising privacy disclosures communicate to users?," *ACM*, 19–30.
- , Ashwini Rao, Florian Schaub, Abigail Marsh, Lorrie Faith Cranor, and Norman Sadeh (2015), "Privacy and Behavioral Advertising: Towards Meeting Users' Preferences."
- Liu, Zhan, Jialu Shan, Riccardo Bonazzi, and Yves Pigneur (2014), "Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications," *IEEE*, 1063–72.
- Malhotra, Deepak (2004), "Trust and reciprocity decisions: The differing perspectives of trustors and trusted parties," *Organizational Behavior and Human Decision Processes*, 94 (2), 61–73.
- and J Keith Murnighan (2002), "The effects of contracts on interpersonal trust," *Administrative Science Quarterly*, 47 (3), 534–59.
- Marotta, Veronica, Kaifu Zhang, and Alessandro Acquisti (2015), "Who Benefits from Targeted Advertising?"
- Marotta-Wurgler, Florencia (2014), "Does 'Notice and Choice' Disclosure Regulation Work? An Empirical Study of Privacy Policies.," *Working Paper*.
- Martin, Kelly D, Abhishek Borah, and Robert W Palmatier (2016), "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing*.
- and Patrick E Murphy (2016), "The role of data privacy in marketing," *Journal of the Academy of Marketing Science*, 1–21.
- Martin, Kelly and Patrick Murphy (forthcoming), "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science*.
- Martin, Kirsten (2012), "Information technology and privacy: conceptual muddles or privacy vacuums?," *Ethics and information technology*, 14 (4), 267–84.
- (2013), "Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online," *First Monday*, 18 (12).
- (2015a), "Privacy Notices as Tabula Rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online," *Journal of Public Policy & Marketing*, 34 (2), 210–27.
- (2015b), "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," *Journal of Business Ethics*, 1–19.
- and Helen Nissenbaum (2016), "Measuring Privacy: Using Context to Expose Confounding Variables," *Columbia Science and Technology Law Review*.
- and Katie Shilton (2015), "Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications," *Journal of the Association for Information Science and Technology*.

- Mayer, Roger C, James H Davis, and F David Schoorman (1995), "An integrative model of organizational trust," *Academy of management review*, 20 (3), 709–34.
- McDonald, Aleecia M and Lorrie Faith Cranor (2008), "Cost of reading privacy policies, the," *ISJLP*, 4, 543.
- McKnight, D Harrison, Vivek Choudhury, and Charles Kacmar (2002), "Developing and validating trust measures for e-commerce: An integrative typology," *Information systems research*, 13 (3), 334–59.
- Milne, George R and Maria-Eugenia Boza (1999), "Trust and concern in consumers' perceptions of marketing information management practices," *Journal of interactive Marketing*, 13 (1), 5–24.
- and Mary J Culnan (2004), "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," *Journal of Interactive Marketing*, 18 (3), 15–29.
- and Mary Ellen Gordon (1993), "Direct mail privacy-efficiency trade-offs within an implied social contract framework," *Journal of Public Policy & Marketing*, 206–15.
- Miyazaki, Anthony D and Ana Fernandez (2000), "Internet privacy and security: An examination of online retailer disclosures," *Journal of Public Policy & Marketing*, 19 (1), 54–61.
- and ——— (2001), "Consumer perceptions of privacy and security risks for online shopping," *Journal of Consumer Affairs*, 35 (1), 27–44.
- Mukherjee, Avinandan and Prithwiraj Nath (2007), "Role of electronic trust in online retailing," *European Journal of Marketing*, 41 (9/10), 1173–1202.
- Nissenbaum, Helen (2004), "Privacy as contextual integrity," *Wash. L. Rev.*, 79, 119.
- (2010), *Privacy in context: Technology, policy, and the integrity of social life*, Stanford University Press.
- and Finn Brunton (2015), *Obfuscation: A User's Guide for Privacy and Protest*, Cambridge, MA: MIT Press.
- Norberg, Patricia A, Daniel R Horne, and David A Horne (2007), "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, 41 (1), 100–126.
- Pavlou, Paul A (2011), "State of the information privacy literature: where are we now and where should we go," *MIS quarterly*, 35 (4), 977–88.
- Pew Research Center (2014a), "Public Perceptions of Privacy and Security in the Post-Snowden Era."
- (2014b), "Net Threats," Pew Research Center.
- (2014c), "Cyber Attacks Likely to Increase," Pew Research Center.
- Rainie, Lee, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish (2013), "Anonymity, privacy, and security online," *Pew Research Center*.
- Richards, Neil M and Jonathan H King (2014), "Big Data Ethics," *Wake Forest Law Review*, 23.
- Riquelme, Isabel P and Sergio Román (2014), "Is the influence of privacy and security on online trust the same for all type of consumers?," *Electronic Markets*, 24 (2), 135–49.
- Roman, Sergio (2007), "The ethics of online retailing: a scale development and validation from the consumers' perspective," *Journal of Business Ethics*, 72 (2), 131–48.
- Román, Sergio and Pedro J Cuestas (2008), "The perceptions of consumers regarding online retailers' ethics and their relationship with consumers' general internet expertise and word of mouth: a preliminary analysis," *Journal of Business Ethics*, 83 (4), 641–56.
- Rossi, Peter H and Steven L Nock (1982), *Measuring social judgments: the factorial survey approach*, Beverly Hills: Sage Publications.
- Schlosser, Ann E, Tiffany Barnett White, and Susan M Lloyd (2006), "Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions," *Journal of Marketing*, 70 (2), 133–48.
- Schumann, Jan H, Florian von Wangenheim, and Nicole Groene (2014), "Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services," *Journal of Marketing*, 78 (1), 59–75.

- Sheehan, Kim Bartel (2005), "In poor health: an assessment of privacy policies at direct-to-consumer web sites," *Journal of Public Policy & Marketing*, 24 (2), 273–83.
- and Mariea Grubbs Hoy (2000), "Dimensions of privacy concern among online consumers," *Journal of Public Policy & Marketing*, 19 (1), 62–73.
- Shultz, Clifford J and Morris B Holbrook (2009), "The paradoxical relationships between marketing and vulnerability," *Journal of Public Policy & Marketing*, 28 (1), 124–27.
- Sirdeshmukh, Deepak, Jagdip Singh, and Barry Sabol (2002), "Consumer trust, value, and loyalty in relational exchanges," *Journal of marketing*, 66 (1), 15–37.
- Smith, H Jeff, Tamara Dinev, and Heng Xu (2011), "Information privacy research: an interdisciplinary review," *MIS quarterly*, 35 (4), 989–1016.
- Solove, Daniel J and Woodrow Hartzog (2014), "The FTC and the new common law of privacy," *Columbia Law Review*, 583–676.
- Soltani, Ashkan, Shannon Canty, Quentin Mayo, Lauren Thomas, and Chris Jay Hoofnagle (2010), "Flash Cookies and Privacy.," 158–63.
- Teufel, Hugo (2008), "The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security," Department of Homeland Security: Department of Homeland Security.
- Toubiana, Vincent, Arvind Narayanan, Dan Boneh, Helen Nissenbaum, and Solon Barocas (2010), "Adnostic: Privacy Preserving Targeted Advertising."
- Trimm, Trevor (2016), "What media companies don't want you to know about ad blockers," *Columbia Journalism Review*.
- Tucker, Catherine (2015), "Economics of Privacy and User-Generated Content," *Emerging Trends in the Social and Behavioral Sciences: An Interdisciplinary, Searchable, and Linkable Resource*.
- Tucker, Catherine E (2012), "The economics of advertising and privacy," *International journal of Industrial organization*, 30 (3), 326–29.
- (2014), "Social networks, personalized advertising, and privacy controls," *Journal of Marketing Research*, 51 (5), 546–62.
- Turow, Joseph, Michael Hennessy, and Nora Draper (2015), "The Tradeoff Fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation.,"
- , Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy (2009), "Americans reject tailored advertising and three activities that enable it," *Available at SSRN 1478214*.
- Ur, Blase, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang (2012), "Smart, useful, scary, creepy: perceptions of online behavioral advertising," in *Proceedings of the 8th Symposium on Usable Privacy and Security*, ACM, 4.
- Vargo, Stephen L and Robert F Lusch (2004), "Evolving to a new dominant logic for marketing," *Journal of marketing*, 68 (1), 1–17.
- Wallander, Lisa (2009a), "25 years of factorial surveys in sociology: A review," *Social Science Research*, 38 (3), 505–20.
- (2009b), "25 years of factorial surveys in sociology: A review," *Social Science Research*, 38 (3), 505–20.
- Warren, Samuel D and Louis D Brandeis (1890), "The right to privacy," *Harvard law review*, 193–220.
- Westin, Alan (2001), *Opinion surveys: What consumers have to say about information privacy*.
- Westin, Alan F (2003), "Social and political dimensions of privacy," *Journal of social issues*, 59 (2), 431–53.
- White, Tiffany Barnett, Thomas P Novak, and Donna L Hoffman (2014), "No Strings Attached: When Giving It Away Versus Making Them Pay Reduces Consumer Information Disclosure," *Journal of Interactive Marketing*, 28 (3), 184–95.
- Xu, Heng, Xin Robert Luo, John M Carroll, and Mary Beth Rossen (2011), "The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing," *Decision Support Systems*, 51 (1), 42–52.

- , Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal (2009), “The role of push-pull technology in privacy calculus: the case of location-based services,” *Journal of Management Information Systems*, 26 (3), 135–74.
- Yang, Sybil and Michael Lynn (2014), “More evidence challenging the robustness and usefulness of the attraction effect,” *Journal of Marketing Research*, 51 (4), 508–13.
- Youn, Seounmi (2009), “Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents,” *Journal of Consumer Affairs*, 43 (3), 389–418.
- Zimmer, Michael (2010), “‘But the data is already public’: on the ethics of research in Facebook,” *Ethics and information technology*, 12 (4), 313–25.

WEB APPENDIX

Table A1: Descriptive Statistics of Surveys 1-4.

	Survey 1		Survey 2		Survey 3		Survey 4	
	Primary Use		Primary + 2nd Use		Primary Use + Security		Primary + 2nd use + Security	
Sample Statistics								
N (Users)	393		381		400		399	
N (Vignettes)	15,720		15,240		16,000		15,960	
DV	-8.47		-16.98		-18.43		-25.23	
SD	28.95		29.46		28.25		27.35	
ICC Null	28.8%		27.1%		26.9%		25.0%	
Respondent R2	0.695		0.744		0.711		0.742	
Respondent Control Variables								
	<u>mean</u>	<u>sd</u>	<u>mean</u>	<u>sd</u>	<u>mean</u>	<u>sd</u>	<u>mean</u>	<u>sd</u>
KnowInternet	2.90	0.97	2.74	0.95	2.86	0.96	2.85	0.93
PrivacyConcern	55.46	40.15	58.21	42.53	59.31	36.98	61.53	38.11
TrustSites	-11.77	48.40	-13.49	48.89	-8.86	49.22	-13.83	48.94
CodingExp	2.07	1.21	2.05	1.15	1.99	1.16	2.10	1.20
PrivacyImportant	78.51	26.47	81.90	24.25	80.07	25.16	82.51	23.07
Gender	1.41	0.49	1.45	0.50	1.45	0.50	1.39	0.49
Age	3.28	1.08	3.31	1.00	3.33	1.11	3.30	1.08

Table A2: Control Variables

Question	Label	Values
Gender	Male	1
	Female	2
Age	Under 18	1
	18-24	2
	25-34	3
	35-44	4
	45-54	5
	55-64	6
	65 +	7
40 Vignettes	<i>I trust this website.</i>	-100...+100
Knowledge Internet <i>How would you judge your knowledge of the technical aspects that make the Internet work?</i>	I don't know any technical details	1
	I have a vague idea of the technical details	2
	I have a good idea of the technical details	3
	I am very knowledgeable	4
	I am an expert	5
Privacy Concern	<i>I am concerned that online companies are collecting too much personal information about me.</i>	-100...+100
Trust in Websites	<i>In general, I trust websites.</i>	-100...+100
Coding Experience <i>How many programming languages have you used for coding?</i>	I have coded in too many languages to count	1
	I have coded in several (2-4) programming languages	2
	I have coded in one programming language	3
	I have coded but do not remember the language	4
	None - I have never coded	5
Privacy Important	<i>In general, I believe privacy is important</i>	-100...+100

Figure A3: Comparison of Trust Rating and Trusting Behavior of Ad Network Player 2

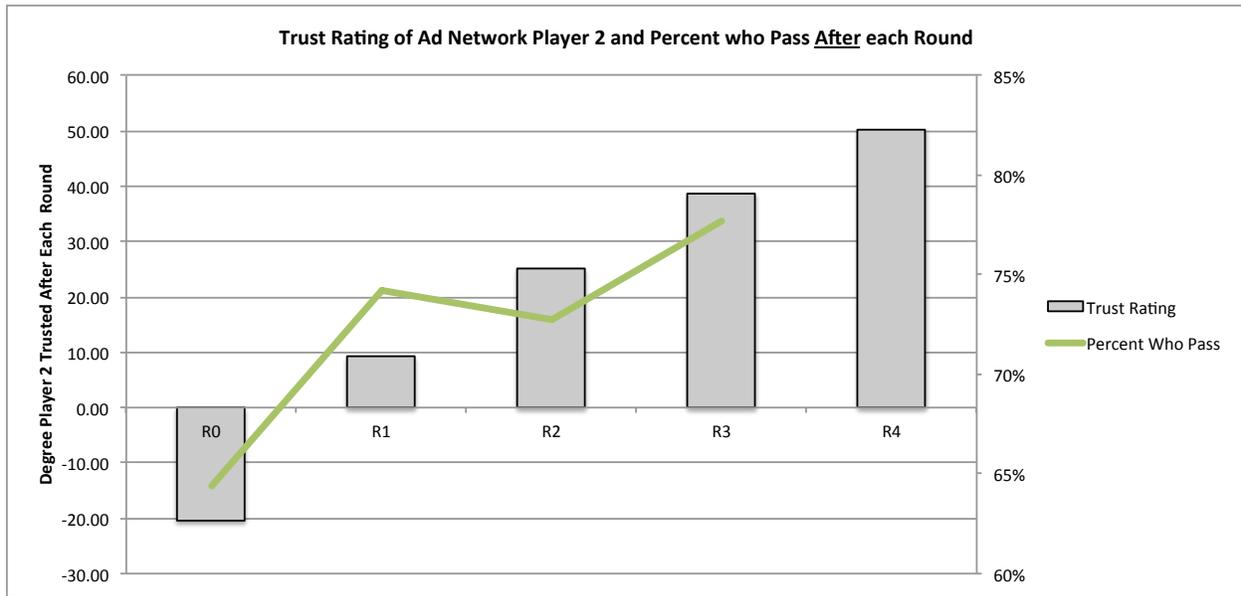


Figure A4: Comparison of Trust Rating and Trusting Behavior of Privacy Preserving Player 2

