How Privacy Flaws Affect Consumer Perception

Sadia Afroz, Aylin Caliskan Islam, Jordan Santell, Aaron Chapin and Rachel Greenstadt
Department of Computer Science
Drexel University

***Abstract*—We examine how consumers perceive publicized instances of privacy flaws and private information data breaches. Using three real-world privacy breach incidents, we study how these flaws affected consumers' future purchasing behavior and perspective on a company's trustworthiness. We investigate whether despite a lack of widespread privacy enhancing technology (PET) usage, consumers are taking some basic security precautions when making purchasing decisions. We survey 600 participants on three well-known privacy breaches. Our results show that, in general, consumers are less likely to purchase products that had experienced some form of privacy breach. We find evidence of a slight bias toward giving products the consumers owned themselves more leeway, as suggested by the endowment effect hypothesis.**

I. Introduction

With the increase of the amount of personal information stored by organizations, privacy and data breaches are becoming more common. These breaches can result in hundreds of thousands (sometimes millions) of lost records, leading to identity theft and related crimes. The public sector response has been increased regulation. United States, for example, has responded by adopting data breach disclosure laws that require firms to notify individuals when their personal information has been compromised [1].

The purpose of such laws is two fold. First, notification directly reduces the harm after the incidence of breach. Once individuals have been notified of the breach, they can begin to take adequate precautions to reduce damage, e.g. by canceling specific credit cards. Second, public disclosure encourages firms to invest in security and privacy technologies by imposing a reputation cost in the market. What is the nature and extent of this reputation cost? Does it influence individual purchasing decisions? Does it impinge individual levels of trust in the company?

Previous investigations of post-breach reputation have only considered the cost to organizations' market value, e.g. stock values [2], [3], [4], [5], [6]. Thus, previous research examined past data and revealed preferences of acceptable risk to end-user from a rational perspective [7]. However, privacy decisions are boundedly rational [8], [9]. E.g., Camp et al. note that for the same level of harm individuals react more strongly to a privacy policy lapse compared to a technical failure [10].

When a company or product experiences a breach of personal information, consumers' perception of the company changes. How the violation occurs, how the company handles the announcement and how they make amends may be critical factors regarding whether or not consumers will choose to do business with that company in the future.

In this paper we plan to study implications of privacy violations beyond stock market impacts and understand how privacy flaws affect the consumers' perception of a company. We performed a survey-based study with 600 participants. We examined consumer perceptions of three companies, namely Apple, Sony and Facebook, after a privacy breach in the corresponding company. The incidents we examined are Apple's iOS location data storage without users' consent, Sony's Playstation Network (PSN) data breach, and changes to Facebook's privacy settings. The main research question we ask is **what is the future implication of a privacy breach from consumers' perspective?** Specifically, we are interested to know:

1) Does a consumer's perception of a company's trustworthiness change over time?
2) Does awareness of a privacy flaw change the consumer's perception of that company's trustworthiness?
3) Does owning a product of a company affect a consumer's perspective after a breach on that company?
4) What type of information breach can cause service termination?

To answer these questions we performed two surveys, once in 2011 and again in 2012. In our results, we did not notice any significant differences in the consumers' perceived trustworthiness of a company immediately after the breach and a year later. But we found a significant relationship between the consumers' awareness of a privacy breach in a company and perceived trustworthiness of that company. We found that in 2011, immediately after the Sony and Apple breaches, consumers who were aware of the breaches perceived the corresponding companies as less trustworthy. But this effect was not found in 2012. We also found that consumers perceive companies like Facebook, where privacy flaws by design are more frequent and publicized, more trustworthy than other companies (Sony and Apple in our case). We noticed an endowment effect when consumers are not reminded of any particular breach. That is people perceive a company as more trustworthy if they own its product. Even after a breach, the endowment effect was significant for iOS owners.

II. Related Work

Considerable research has been done to understand the cost of privacy breaches on an organization's market value [2], [3], [4], [5], [6]. Acquisti et al.'s seminal study on the cost of privacy breaches discussed the impact of privacy breaches on a company's market value [2]. Their analyses showed that on the day of the breach a company's market value decreases significantly but the significance diminishes in the following days. Campbell et al. found that the stock price of companies reporting a security breach is more likely to fall if the breach leaked confidential information [11].

Previous research also considered market behavior as a proxy for individual preferences. This methodology for understanding consumer perceptions is known as revealed preferences [12]. There are, however, several limitations. First, revealed preferences does not account for network effects, e.g. lock-in. Secondly, revealed preferences notes risk levels that have been accepted in the past but does not illuminate what is desirable from a consumer's perspective. The alternative approach is expressed preferences that survey consumers to elicit individual perspectives [13].

For example, the Ponemon Institute performed several surveys on American consumers to understand consumers' perceptions and concerns about data breaches after receiving notification [14]. Their studies note that consumers lose confidence in firms that suffer breaches and that consumers' perspective depends on the benefit offered to them after the breach. Consumers are more favorable to the organization if they receive free or subsidized services as a consequence of the breach.

Arguably, information about the privacy risk informs individual decisions. Tsai et al. showed that accessible privacy information can change consumers' purchasing behavior by making them choose online retailers with better privacy policies [15]. Specific characteristics of the risk also inform perceptions. For example, when the consequences of an activity are perceived as controllable, individuals are more accepting of risk [16]. The most important determinant of risk, however, is the perceived severity of consequences [17].

Previous survey based research has not considered questions of availability [18]. Arguably, when information is easier to recall, perceptions are more informed [19]. Prior work also does not consider the difference in perceptions based on individuals affiliation with the brand suffering repetitive consequences of the privacy breach. Individual privacy decisions are boundedly rational [8], [9] and thus are impinged by cognitive biases such as the endowment effect [20]. Finally, privacy preferences are contextual [21]. Thus, not all risks would be similarly informed. The nature of the privacy violation, e.g. whether it is a one time violation vs. an ongoing property of the system, could elicit different end-user preferences.

In this study, we examine both of these effects immediately after a breach and also a year later. We also examine the differences between individuals who own the specific product or service under consideration. We consider three distinct breaches to account for contextual differences.

III. The Privacy Flaws

We polled consumers on three privacy breach incidents: a privacy flaw in Apple's iOS location data storage, Sony's Playstation Network (PSN) data breach, and the 2009 changes to Facebook's privacy settings. We chose these breaches because of their contextual differences and consumers' familiarity with the incidents. Different kinds of breaches are chosen to generalize consumers' opinion on private data exposure. All the three breaches were reported in the mainstream media. Out of the three incidents, the PSN breach was the only instance where user data was actually stolen; in the other two cases, private data were exposed because of poor privacy by design.

Apple iOS Location Data Storage.: Apple's iOS4 operating system (found on iPhones and iPads) had a privacy vulnerability that logged locations (latitude, longitude, and timestamp) of cell-towers and WiFi hotspots on a file (consolidated.db) regardless of whether or not the location based services have been enabled. This flaw was publicized on April 20, 2011 [22]. The consolidated.db file was stored unencrypted on an iOS4 device's filesystem since the day the operating system was installed and was copied to any computer the device synced with, leaving behind copies of unencrypted data about where the user has been with their iPhone or iPad. This issue was present before the release of iOS4 and known to forensics teams and researchers [23]. Allan and Warden's iPhone Tracker tool publicized it by visualizing device locations from the the consolidated.db on a map [24].

Facebook's Default Privacy Settings.: In December 2009, Facebook changed their user privacy policy requiring all users to utilize a "privacy transition tool." This tool by default left many previously protected pieces of information available for consumption by the general public. Before the changes, a user had the option of exposing only a "limited" profile, consisting of as little as his name and networks, to other Facebook usersand nothing at all to Internet users at large. But after the change profile picture, current city, friends list, gender, and fan pages are "publicly available information." [1] The tool did not allow most users to strengthen privacy settings.

Sony's PlayStation Network Breach.: In April 2011, soon after the iOS flaw was announced, 77 million accounts of Sony's Playstation Network (PSN) had been breached, followed by another Sony system compromise, leading to a total of over 100 million user accounts being affected[2]. The data stolen included names, addresses, e-mail addresses, birthdays, passwords, "secret questions" and their respective answers. It was not known whether or not credit card data had also been stolen, but evidence suggested that it had not been compromised. One reason that the infiltration was successful that two to three months before the breach, Sony employees posted information on an open forum stating that their systems were running an out-of-date and unpatched version of the Apache Web Server, and operated without any form of firewall.

IV. Hypotheses

Previous studies showed that a company's stock value decreases significantly whenever a breach is announced but the significance diminishes in the following days [2]. As such, the stock value of a company is an indicator of the market's trust in the company. If the trust of the market follows individual trust in a company, we would expect to see a similar impact on the company's trustworthiness.

H1: *Consumer perceptions of a company's trustworthiness a year after the breach should be higher than immediately*

[1]Facebook Privacy in Transition - But Where Is It Heading?: https://www.aclunc.org/issues/technology/blog/facebook_privacy_in_transition_-_but_where_is_it_heading.shtml

[2]Play by Play: Sony's Struggle on Breach: http://online.wsj.com/article/SB10001424052748704810504576307322759299038.html

after the incident.

Availability heuristic refers to the ease with which an individual can retrieve an instance of, for example, an incident. For example, there are more words with 'r' as the third letter than words that begin with r. However, it is much easier to recall the latter. Thus, individuals often assume that there are more words that begin with 'r'. Thus, availability impinges individual's ability to imagine the probability of risk. For example, individuals who see pictures of floods assume a higher probability of being flood victims themselves [25]. Similarly online individuals who are more aware of privacy breaches should arguably perceive a higher risk of information sharing. Thus, individuals with more awareness should have lower levels of trsutworthiness.

H2: *Consumers who are aware of privacy breaches will perceive the company as less trustworthy.*

Ownership of a product or subscription to a service would also impinge individual perceptions of trust. Typically, individuals value more what they already own. For example, for the same piece of information individuals assign a higher value when the information is being sold than when it is being protected [20]. This is called the endowment effect. Does the monetary notion of endowment transfer to non-monetary notions of value like trust? Assuming it does we expect that consumers who own a company's product will not lose trust in that company after a breach.

H3: *Consumers who own the product will perceive the company to be more trustworthy after the breach, compared to consumers who don't.*

In addition to these hypotheses, we study other aspects of breaches:

1) How a breach affects a consumer's future usage and purchasing behavior?
2) What kind of breach would cause service termination?

V. Methodology

A. Survey Design

We conduct two distinct surveys. The first survey elicits consumers' general perceptions of Apple, Sony and Facebook. The second survey addresses how consumer perceptions change after learning about privacy breach. The purpose of the first survey is to understand consumers' trust, usage patterns, and future purchasing behavior without reminding them about privacy leaks. The goal of the second survey is to understand four issues regarding changes in consumer perception because of a privacy leak: (1) changes in usage pattern, (2) changes in trustworthiness of the relevant company, (3) importance of different data, and (4) the endowment effect.

Our surveys consist primarily of quantitative questions, using either binary yes/no responses or Likert-scales. There are four sections in the first survey: Demographic Information, Perception about Apple, Sony, and Facebook. In the Demographic Information section, participants are asked questions about their demographics, for example, gender, age, education level, yearly income along with the kind of phone, online gaming network and social network they use. The following three sections consist of questions regarding future usage, trustworthiness of the three companies, likeliness of an information breach, and whether participants were aware of any past breaches that happened to these companies.

The second survey has five sections: Demographic Information, iOS Privacy Breach, Playstation Network breach, Facebook Privacy Settings, and General. The demographic section is similar to the first survey. The next three sections consist of questions regarding a specific privacy breach. In each of these sections, we first determine the respondent's awareness of the issue. We provide a brief summary of each of the privacy flaws, giving enough information to the respondent so that they could provide informed responses to the later questions. We then ask questions regarding the importance of data to a consumer and what kind of data breach would cause them to stop using a service or product.

We conduct the second survey twice 16 months apart, once in June 2011, right after the iOS and PSN breach happened and again in October 2012. Our purpose for doing this is to follow up with the change in consumer's perspective over time.

B. Data Collection

To gather a wide variety of respondents, we used Amazon's Mechanical Turk service. We collected demographic information from respondents, as well as their results, to verify that a single age or income level is not over-represented in our results. The use of Mechanical Turk does imply some level of technical competency, as Turkers need to deal with the intricacies of the Mechanical Turk system.

TABLE I: **Demographics**

	Male	**Female**	**Average age**	**Education***
2011	53%	47%	30.21	87.5 %
2012	61.5%	38.5%	30.46	90.5%
General Survey	70.5%	29.5%	30.775	94.5%

*Percentage of participants with at least some college education

Using this system, we collected 200 responses on the first survey and total 400 responses on the second survey: 200 responses in June 2011 and 200 responses in October 2012. In total we collected data from 600 respondents, 61.67% of them were male, and 38.33% were female (details are shown in Table I). The average age of the respondents was around 30, and although the majority of the respondents skewed toward the younger demographics, there was a representation of ages from 18 to 66.

Each respondent was required to have either an iOS device, PSN, or Facebook account. We asked whether or not the respondents with Facebook accounts had been members during the time period of the privacy change in 2009, but we did not require it.

VI. Results

We noticed that the data we collected were not normally distributed but heavily skewed for the most part. So we used

TABLE II: Differences between survey population in 2011 and 2012: This table shows differences in some variables between the survey population. Except in education, there were no significant differences between the survey population in 2011 and 2012.

Variable	P-value
Gender	0.47
Age	0.76
Education	0.006**
Income	0.23
Whether or not own Apple	0.18
Whether or not own other smart phone	0.07
Whether or not use PSN	0.66
Whether or not use other game service	0.51
Whether or not use Facebook	≈1
Whether or not use other social network	0.15
Apple: Awareness of iOS devices' location storage	0.13
Apple: Awareness[3]	0.05
Apple: Perceived trustworthiness	0.17
Sony: Awareness of PSN data breach	0.32
Sony: Awareness of outdated Software package	0.90
Sony: Perceived trustworthiness	0.17
Facebook: Awareness of privacy Settings Available	0.98
Facebook: Perceived trustworthiness	0.40
General: Privacy concern in entertainment service	0.69
General: Privacy concern in technological necessity	0.92
General: Privacy concern in financial service	≈0 ***

non-parametric tests to determine statistical significance. For comparing means we used the Mann-Whitney test or the Wilcox Test. Means were used to compare interval or ratio variables. For testing proportions, we used Fisher's test for nominal binary variables and a chi-squared test for ordinal variables. The results shows that the survey population in 2011 and 2012 were statistically similar (shown in Table II). The only difference was in terms of education. We also calculated the correlation between perceptions and the different independent variables. We used Kendall's Tau (τ) for ratio, interval, and ordinal data. When one of the variables is dichotomous, we calculated the point biserial correlation. The values were the same as for Kendall's Tau. Henceforth we will just use Kendall's Tau. The results are shown in Tables III and IV.

A. General Perception

We asked users about their general perception about Apple, Sony and Facebook without telling them anything about the breaches. In particular we asked users to rate their likeliness of future purchase or usage, trustworthiness of the company, likeliness of a data or privacy breach happening and whether they are aware of any past breach. The majority of the users had very positive opinion of these three companies before knowing about the breach incidents.

Most users, over 70% for Apple and Sony and 48.5% in case of Facebook, perceived these companies' trustworthiness as above average and majority of them were unaware of any past breaches (shown in Table V). For all three companies,

TABLE III: Correlations with perceived trustworthiness: 2011. Single star represents significance at the 0.5 level and double star represents 0.01 level significance.

Variable	Apple	Sony	Facebook
Gender	0.14*	0.20**	0.06
Age	-0.02	-0.10	-0.16*
Education	0.07	0.06	0.06
Income	-0.08	-0.18	-0.18
Whether or not own Apple	-0.15*		
Whether or not own other smart phone	0.02		
Whether or not use PSN		-0.07	
Whether or not use other game service		-0.02	
Whether or not use Facebook			0.03
Whether or not use other social network			-0.02
Apple: Awareness of the breach	0.18**		
Apple: Awareness of information collection without explicit consent	0.11		
Apple: Awareness of data saved to iOS devices	0.22**		
Apple: Awareness of easy accessed to location data	-0.14*		
Apple: Consumers' concern about the data collection	-0.09		
Sony: Awareness of PSN data breach		0.002	
Sony: Awareness of outdated software package		0.16*	
Facebook: Awareness of privacy settings available			0.26***

TABLE IV: Correlations with perceived trustworthiness: 2012. Single star represents significance at the 0.5 level and double star represents 0.01 level significance.

Variable	Apple	Sony	Facebook
Gender	0.005	-0.08	-0.12
Age	0.07	-0.04	0.03
Education	0.13*	0.09	0.07
Income	-0.14*	-0.21***	-0.08
Whether or not own Apple	-0.09		
Whether or not own other smart phone	-0.01		
Whether or not use PSN		-0.12	
Whether or not use other game service		-0.13*	
Whether or not use Facebook			0.05
Whether or not use other social network			0.10
Apple: Awareness of the breach	-0.17**		
Apple: Awareness of information collection without explicit consent	-0.13*		
Apple: Awareness of data saved to iOS devices	-0.27***		
Apple: Awareness of easy accessed to location data	0.17**		
Apple: Consumers' concern about the data collection	0.27***		
Sony: Awareness of PSN data breach		0.06	
Sony: Awareness of outdated software package		-0.21**	
Facebook: Awareness of privacy settings available			0.33***

TABLE V: **General perception of Apple, Sony and Facebook**

	Usage	Trustworthiness	Likeliness Future Breach	Awareness of Past Breach	Future Usage
Apple	61.5%	76.5%	14%	26%	93%
Sony	57%	73.5%	27%	31.5%	82%
Facebook	97.5%	48.5%	39%	52%	85.5%

consumers who were not aware of any past breaches perceived the companies as significantly more trustworthy (Apple: p-value=0.0004, τ=0.23; Sony: p-value=0.02,τ=0.14; Facebook: p-value=0.00003, τ=0.23). Also, in case of Apple and Sony, people who owned their product trusted them significantly more than people who did not own product (with p-value $<$ 0.005). People who trusted the companies are more likely to use their products in future (p-value $<$ 0.005).

B. Awareness

We asked the participants whether or not they are aware of the particular privacy breaches described in section 3. In 2011, 54% of the participants were aware of the Apple iOS storage flaw before taking our survey (Table VI). There was no statistically significant awareness difference between 2011 and 2012 (Table II). 60.5% of the participants were familiar

TABLE VI: **Initial Awareness of the Breaches**

	Usage (2011)	Awareness (2011)	Usage (2012)	Awareness (2012)
Apple iOS	46%	54%	58.5%	57%
Sony PSN	42%	60.5%	44.5%	55.5%
Facebook	95.5%	70%	96.5%	70%

with the PSN breach in 2011 which decreased to 55.5% in 2012 in spite of 2.5% increase in usage. Unsurprisingly, a strong majority (95.5% in 2011 and 96.5% in 2012) of our respondents are Facebook users, 70% of whom were aware of the default privacy settings.

C. Effect on trustworthiness

We asked participants to rate on a 5-point Likert scale how revelation of the breach affected their perception of corresponding organizations trustworthiness.

We noticed that for Apple, consumers who were aware of the breach lost their trust immediately after the breach. In 2011, 59% of the participants perceived Apple as less trustworthy because of the breach (Figure 1). We also asked consumers about specific details of the breach to understand what was most important to them. In particular, we asked whether or not they were aware that: 1) the data was collected without explicit consent (even when the device is set not to collect location information), 2) when an iOS device syncs to any computer, the unencrypted location files was stored on that computer and 3) anybody can download and access the location data from an iOS device. There were no significant relationship between trustworthiness and data collection. The individuals who knew about the data sync found Apple as significantly less trustworthy (with p-value $<$ 0.01), as shown in Table III.

In 2012 the construct of trustworthiness changes. Consumers who were aware of the breach in 2011 perceived Apple as more trustworthy (p-value $<$ 0.01), as shown in Table IV. Individuals concerns were about data collection itself and perceived Apple as significantly more trustworthy when they were aware of the details of the breach.

For Sony, 67% of the participants' perceived Sony as less trustworthy after the breach in 2011 (Figure 2), though this change was not statistically significant. In 2011, Individuals who knew about the outdated package trusted Sony less (p-value $<$ 0.5). Again in 2012 the construct of trustworthiness changes. Individuals who knew about the outdated package trusted Sony more (p-value $<$ 0.01).

In Facebook's case majority of the participants perceived Facebook as more trustworthy in both 2011 and 2012 (Table VII). Here those who knew that access for privacy settings was public by default trusted Facebook significantly more (p-value $<$ 0.001).

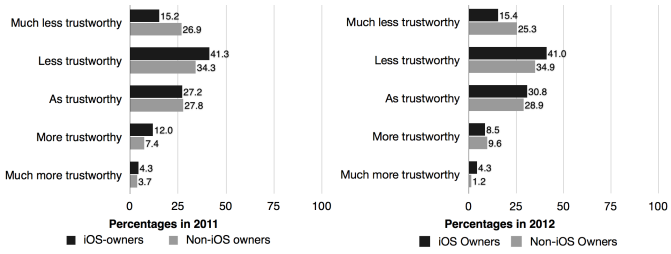

Fig. 1: **Effect on Apple's trustworthiness due to privacy breach**: iOS owners perceived Apple as significantly less trustworthy in 2011 and more trustworthy in 2012

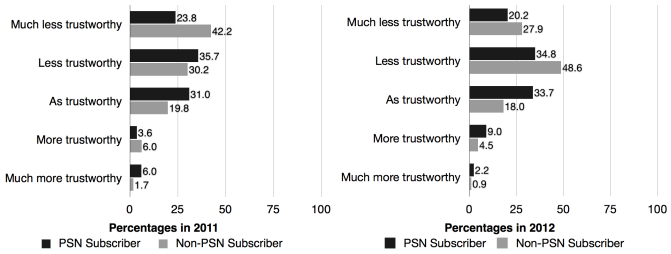

Fig. 2: **Effect on Sony's trustworthiness due to privacy breach**: PSN subscribers perceived Sony as slightly less trustworthy in 2011 and more trustworthy in 2012

TABLE VII: **Effect on Facebook's Trustworthiness**: Facebook users who were aware of the default privacy settings perceived Facebook as more trustworthy in both 2011 and 2012.

	% Responses (2011)	% Responses (2012)
Much less trustworthy	16%	24%
Less trustworthy	31%	31.5%
As trustworthy	43%	36%
More trustworthy	5%	6%
Much more trustworthy	5%	2.5%

D. Effect on usage and purchasing behavior

1) Future iOS/Apple Purchases.: Figure 3 and 4 show consumers' future purchasing inclination of iOS and Apple products, respectively. Non-iOS users reported being less likely

to purchase an iOS device in the future (55.1% on average) compared to current iOS owners (48.65% on average). Current iOS owners were significantly more likely to buy iOS devices in future ((p-value = 0.01, τ=-0.15). Being already invested in the iOS brand, they are less likely to want to switch. While this may be a motivator for some, the group of iOS owners was still split almost in half, so the endowment effect may not be a particularly powerful motivator.

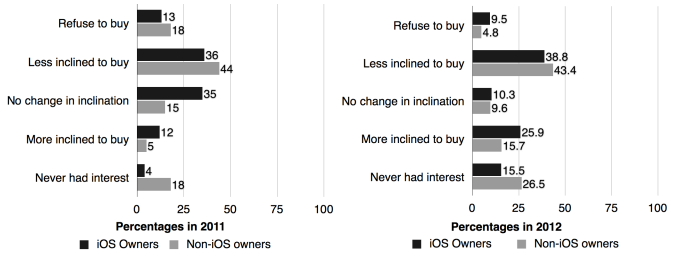

Fig. 3: **Future iOS Purchase Inclination, by iOS and non-iOS owners**: iOS owners are more likely to buy iOS devices in future.

Similar behavior carried over to Apple products in general, as 57% of non-iOS owners stated they are less likely to purchase any Apple product in the future due to the flaw, shown in Figure 4. Majority iOS owners (55%) stated that they are more likely to buy Apple products (p-value = 0.23, τ = -0.07). As a whole, potential future sales of iPads and iPhones were more hurt than their creator's other products, but only by 4% (iOS owners) and 5% (non-iOS owners).

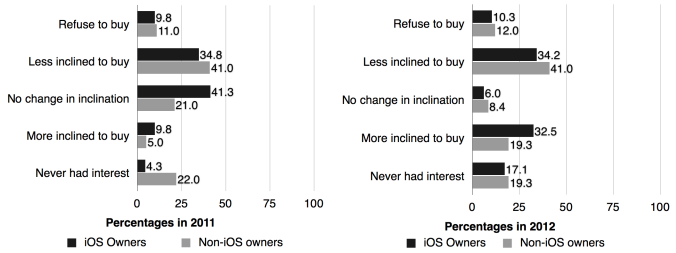

Fig. 4: **Future Apple Product Purchase Inclination, by iOS and non-iOS owners**: iOS owners are more likely to buy Apple products in future.

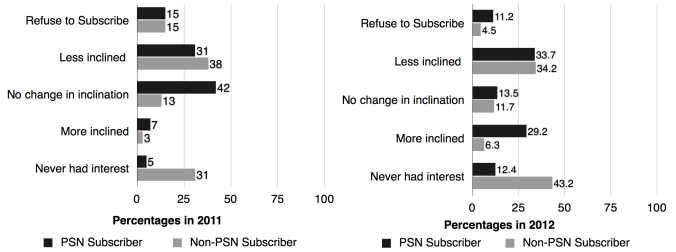

Fig. 5: **Future PSN Subscription Inclination, by PSN and non-PSN subscriber**: PSN subscribers are more likely to use PSN service in future.

2) Future PSN/Sony Purchases: Figure 5 and 6 show future usage inclination of PSN/Sony products. Non-PSN users (53%) are less likely to subscribe to the network after the breach than current PSN subscribers (46%). Sony's potential future sales were also damaged. 46% of the PSN subscribers and 49% of non-PSN users were less likely to purchase Sony products in the future (Figure 6). PSN subscribers were slightly more favorable toward PSN and sony than non subscribers (p-value = 0.27, τ = -0.07). The smaller disparity between users and non-users compared to Apple's potential loss could be attributed to Sony's wide array of products, with the Playstation Network only accounting for a small niche, compared to Apple's more focused market.

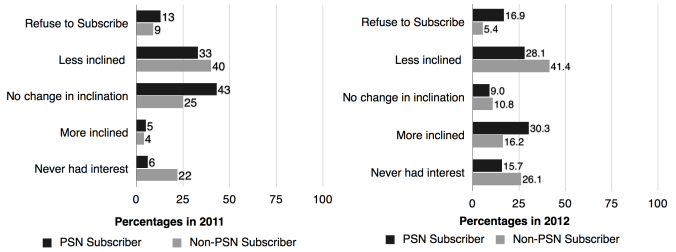

Fig. 6: **Future Sony Purchases Inclination, by PSN and non-PSN subscriber**: PSN subscribers are more likely to buy/use Sony products in future.

3) Future Facebook/Social network usage.: Even knowing about the privacy flaw, 56% of the participants did not change their Facebook usage (shown in Table VIII). Only 9% people refused to use Facebook after knowing about the flaw.

TABLE VIII: **Effect in Facebook Future Usage**

	% Responses (2011)	% Responses (2012)
Planning on using Facebook	56.5%	54%
Was not planning on using Facebook	6%	5%
Less likely to use Facebook	18.5%	22%
More likely to use Facebook	10%	15%
Refuse to use Facebook	9%	4%

TABLE IX: **Effect in Social Network Future Usage**

	% Responses (2011)	% Responses (2012)
Planning on using	52%	44.5%
Was not planning on using	6%	10%
Less likely to use	23.5%	22%
More likely to use	11%	10%
Refuse to use	7.5%	13.5%

We also asked how this information affected respondent's willingness to participate in any social networking sites. In 2011, a similar number of people (52%) said they would continue to use social networking sites, however these numbers dropped in 2012 (Table IX).

E. Endowment effect

Endowment effect is a well-known hypothesis in behavioral economics [26] that suggests that people tend to value the things they own more than things they do not. Being less invested in the company or brand, consumers could be harsher as they were not casting aspersions on their own purchases. On the other hand, owners of products that revealed a privacy breach might be more upset than non-owners, as they were directly affected. We want to understand which effect has a stronger role in consumers' decisions: Are their opinions more

affected by the endowment effect or by owning a product with a privacy breach and having their own data at risk?

Statistically, we noticed iOS owners perceived Apple as significantly more trustworthy immediately after the breach (p-value = 0.01, τ=-0.15), though the significance disappeared in 2012. iOS owners were also more likely to buy iOS devices and other Apple products in future (p-value = 0.01, τ = -0.16). The PSN subscribers were also slightly more likely to use PSN in the future than non-PSN owners (p-value = 0.27, τ = -0.07).

We also looked at their "harshness" compared to both products. We compared each user's response to whether they would purchase iOS products in the future to whether they would subscribe to PSN in the future. If the difference in these values was zero, it indicated that the respondent felt the same way about both products. A divergence in either direction would suggest that they were either more harsh to a certain product, or favored the other. To observe bias, we split the respondents into four groups: those who were iOS users, but not PSN subscribers, those who were PSN subscribers, but not iOS users, those who were both, and those who were neither.

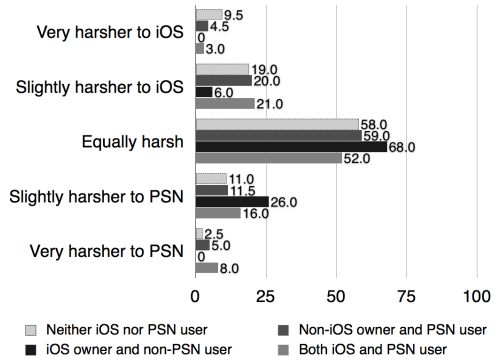

Fig. 7: **% of consumers perspective on product harshness due to privacy breach**

A majority of all four groups were equivalent in their opinion about both products (shown in Figure 7). Users of iOS, but not PSN, had the largest majority (68%) of those who viewed the companies in the same light, though that group was the harshest toward PSN (26%). Users of both platforms were the most divergent group, even with 52% having the same opinion on both. This group was also the most harsh toward Apple, with a combined group of 27% having negative feelings, some very strong, about the iOS. Those who were PSN users but not iOS users, were fairly balanced, but slightly harsher toward PSN than to iOS. Those who were users of neither product were also fairly divided.

F. Severity of different breaches

We wanted to understand what kind of breach would make a user stop using a service or product. We asked this question in regards to three kinds of services: Entertainment, technology and financial. The data type users were asked to consider are: only generic (name, date of birth, etc.), some personal (address, marital status, etc.), and very personal (credit card, SSN, etc.). Figure 8 shows users' responses in 2011 and 2012. The majority of the users would stop using a service if their credit card number or SSN were accessed because of the breach.

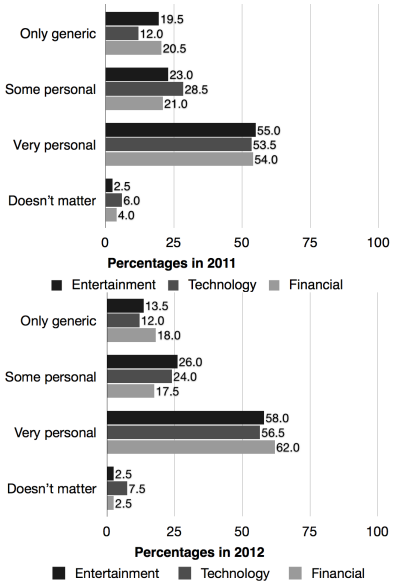

Fig. 8: **What kind of data breach can cause service termination? a) response in 2011, b) response in 2012**

We noticed around a 4% increase in user concern regarding their very personal information (credit card, SSN) and 8% increase in case of using financial services from 2011 to 2012 (p-value $\approx$ 0). Overall, users are becoming more concerned about their data privacy than before.

VII. Discussion

In this section we discuss the questions we posed at the beginning of the paper along with the hypotheses.

Does a consumer's perception of a company's trustworthiness change over time? Our first hypothesis was that consumers will lose trust in a company immediately after a breach, but trust will attenuate over time. In our survey, we did not notice any significant differences in trustworthiness from 2011 (immediately after the breaches) to 2012. However, while in 2011 trustworthiness was related with awareness, ownership or brand affinity, in 2012 these factors might depend on company's reaction after the breaches happened.

Does awareness of a privacy flaw change the consumer's perception of that company's trustworthiness? We expected individuals who knew more about the privacy breaches to have lower levels of trust. When consumers were not reminded of any particular privacy breach, they perceived the companies' trustworthiness as above average. When reminded of some particular breaches, timing effect was evident. For Sony and Apple, we noticed aware consumers lost trust in the companies immediately after the breach but effect disappeared a year later. For Facebook, we noticed an opposite effect, aware consumers trusted Facebook more. One possible explanation could be that as the number of breaches in a company grows, a "privacy fatigue" might emerge [2] and consumers no longer trust a company only based on publicized privacy flaws.

Does owning a product of a company affect a consumer's perspective after a breach on that company? When consumers were not reminded of any particular privacy breach,

significant number of product owners perceived the companies' trustworthiness as above average. Even after knowing about the breach, iOS owners in 2011 perceived Apple as more trustworthy. PSN subscribers were also found Sony as more trustworthy, but that effect was not significant. This finding supports our third hypothesis that consumers tend to trust companies whose products they own.

What type of information breach can cause service termination? Majority of the consumers responded that they would stop using service if financial information was exposed.

Effect on overall brand. In general, consumers who trusted a company more were more likely to buy or use that company's product. Even after a breach, people who trusted Apple and Sony were more likely to buy the corresponding company's products (Apple: p-value = 0.007, τ = 0.16; Sony: p-value $\approx$ 0, τ= 0.28). We found that despite the differences in the iOS and Sony breaches, consumers overwhelmingly viewed them in a similar light. The iOS issue had no reported incident of actually compromising any user's private data, and was guilty primarily of not informing the user about data collection. In the PSN breach, millions of user accounts were stolen by an unauthorized party, due in a large part to mistakes made by the company. However, the majority of the public feels the same way about both these incidents. This conclusion should be of particular concern to business owners. It emphasizes the need for communication of intention to consumers regarding privacy issues. If users even feel that there may be a breach of privacy, that perception to them is almost as bad as if a full-scale breach had occurred.

Limitations. The numbers provided in our survey are self-reported and the subject's true feelings and behaviors cannot be verified. Previous research has shown dichotomy in consumers' privacy concerns in surveys with their actual purchasing/usage behavior [27]. Our survey population is limited to Turkers and they have at least basic understanding of technology and Internet usage. If we conduct the surveys via mail or phone, the population and the opinions might be different.

VIII. Conclusion

Products with privacy breaches impose a prominent effect on the way consumers view the product and its brand. In this work we surveyed users about their perception of three companies, Apple, Sony and Facebook, after learning about the privacy flaws in these companies. Our result shows that consumers aware of the privacy flaws trust a company less. We also show due to the endowment effect the strongest hit from the privacy breach is on the potential customers. The knowledge of how privacy breaches affect consumers is important as it can help researchers design better privacy enhancing technologies and companies to protect their brands' trustworthiness, products' success and market value.

Acknowledgement

We want to thank Vaibhav Garg for his help with the statistical analysis and feedback on improving the paper. We also thank the anonymous reviewers for their helpful comments. We are grateful to the Intel Science and Technology Center (ISTC) for Secure Computing for supporting this work.

References

[1] : State security breach notification laws. http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx (2012)
[2] Acquisti, A., Friedman, A., Telang, R.: Is there a cost to privacy breaches? an event study. In: Fifth Workshop on the Economics of Information Security. (2006)
[3] Andoh-Baidoo, F., Osei-Bryson, K.: Exploring the characteristics of internet security breaches that impact the market value of breached firms. Expert Systems with Applications **32**(3) (2007) 703–725
[4] Cavusoglu, H., Mishra, B., Raghunathan, S.: The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce **9**(1) (2004) 70–104
[5] Garg, A., Curtis, J., Halper, H.: Quantifying the financial impact of it security breaches. Information Management & Computer Security **11**(2) (2003) 74–83
[6] Gatzlaff, K., McCullough, K.: The effect of data breaches on shareholder wealth. Risk Management and Insurance Review **13**(1) (2010) 61–83
[7] Garg, V.: Cars, condoms, and risk perceptions. IEEE Security and Privacy Magazine (2013)
[8] Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. Security & Privacy, IEEE **3**(1) (2005) 26–33
[9] Garg, V., Camp, L.J.: Heuristics and biases: Implications for security and privacy. IEEE Technology and Society (2013)
[10] Camp, L.J., McGrath, C., Genkina, A.: Security and morality: A tale of user deceit. Models of Trust for the Web (MTW06), Edinburgh, Scotland **22** (2006)
[11] Campbell, K., Gordon, L., Loeb, M., Zhou, L.: The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security **11**(3) (2003) 431–448
[12] Starr, C.: Social benefit versus technological risk. Science **165**(3899) (1969) 1232–1238
[13] Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B.: How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. Policy Sciences **9**(2) (1978) 127–152
[14] Ponemon, L.: Consumers report card on data breach notification. Technical report, Technical report, Ponemon Institute (2008)
[15] Tsai, J., Egelman, S., Cranor, L., Acquisti, A.: The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research **22**(2) (2011) 254–268
[16] Brandimarte, L., Acquisti, A., Loewenstein, G.: Misplaced confidences: Privacy and the control paradox. Social Psychological and Personality Science (2012)
[17] Garg, V., Camp, J.: End user perception of online risk under uncertainty. In: System Science (HICSS), 2012 45th Hawaii International Conference on, IEEE (2012) 3278–3287
[18] Tversky, A., Kahneman, D.: Availability: A heuristic for judging frequency and probability. Cognitive psychology **5**(2) (1973) 207–232
[19] Garg, V., Camp, L., Connelly, K., Lorenzen-Huber, L.: Risk communication design: video vs. text. In: Privacy Enhancing Technologies, Springer (2012) 279–298
[20] Grossklags, J., Acquisti, A.: When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In: Workshop on the Economics of Information Security (WEIS). (2007)
[21] Nissenbaum, H.: Privacy in context: Technology, policy, and the integrity of social life. Stanford Law Books (2009)
[22] Allan, A., Warden, P.: Got an iphone or 3g ipad? apple is recording your moves. OReilley Radar (2011)
[23] Levinson, A., Stackpole, B., Johnson, D.: Third party application forensics on apple mobile devices. In: System Sciences (HICSS), 2011 44th Hawaii International Conference on, IEEE (2011) 1–9
[24] CAHILL, K.: Apple iphone tracking your every move? (2011)
[25] Keller, C., Siegrist, M., Gutscher, H.: The role of the affect and availability heuristics in risk communication. Risk Analysis **26**(3) (2006) 631–639
[26] Kahneman, D., Knetsch, J., Thaler, R.: Experimental tests of the endowment effect and the coase theorem. Journal of political Economy (1990)
[27] Acquisti, A., Grossklags, J.: Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In: 2nd Annual Workshop on Economics and Information Security-WEIS. Volume 3. (2003)