The findings of our experiments showed that social network sites (SNSs) such as Google Plus, Facebook, and Twitter, have the ability to acquire knowledge about their users' movements not only within SNSs but also beyond SNS boundaries, particularly among websites that embedded SNS widgets such as Google’s Plus One button, Facebook’s Like button, and Twitter's Tweet button. In this paper, we analysed the privacy implication of such a practice from a moral perspective by applying Helen Nis ...
Contextual Integrity’s decision heuristic and social network sites tracking

Author 1 · Author 2

Received: date / Accepted: date

Abstract The findings of our experiments showed that social network sites (SNSs) such as Google Plus, Facebook, and Twitter, have the ability to acquire knowledge about their users’ movements not only within SNSs but also beyond SNS boundaries, particularly among websites that embedded SNS widgets such as Google’s Plus One button, Facebook’s Like button, and Twitter’s Tweet button. In this paper, we analysed the privacy implication of such a practice from a moral perspective by applying Helen Nissenbaum’s decision heuristic derived from her Contextual Integrity framework in order to answer the question of whether or not an online user’s privacy is being violated by this practice.

Keywords Social networking sites · privacy · online tracking · decision heuristic · contextual integrity framework

1 Introduction

Philosophical accounts of privacy are not empirically-based and technical accounts of privacy do not explain why privacy matters, or what is wrong with breaching it on moral grounds. This article capitalises on the strengths of both approaches. The article reports on a study that examined the implications on privacy from the practice of tracking online users’ movements across different sites by three social networking site (SNS) companies via the use of their widgets (Facebook’s Like button, Twitter’s Tweet button, and Google’s Plus One button).

SNSs have attracted the attention of dozens of researchers from different discipline areas. In addition to contributing to our knowledge of the nature and impacts of SNSs, their interest has been in examining the issue of privacy in SNSs. There are many empirical studies conducted in the SNS area that focus
on users’ informational privacy and what pieces of users information are being shared on the internet with and without users awareness and consent (e.g., [Charnigo and Barnett-Ellis(2007)], [Pempek et al(2009)], [Pempek, Yermolayeva, and Calvert], [Krishnamurthy and Wills(2010a)], [Krishnamurthy and Wills(2010b)], [Mayer(2011)], [Krishnamurthy and Naryshkin(2011)], to name a few). However, to our knowledge, few of these studies provided an interpretation of the research findings from a moral perspective. On the other hand, many philosophical works that examined privacy on moral ground are seen to rely only on thought experiments which are sometimes charged with being unrealistic and bearing little or no relation to real life [Lucas and Mason(2008)]. We believe that analysing an issue from a philosophical perspective should be supported by the results of empirical research. This article provides a philosophical perspective to the issue of tracking in SNSs on the basis of an empirical study that we conducted in 2012.

Contextual Integrity (CI) has been used to analyse privacy online in several contexts, for example, in the context of public records online, and the radio frequency identification (RFID) [Nissenbaum(2004)], data mining [Nissenbaum(2004)], [Tavani(2007)], blogosphere [Grodzinsky and Tavani(2010)], cloud computing [Grodzinsky and Tavani(2011)] and Facebook’s News Feed feature [Hull et al(2011)]. This work will employ the decision heuristic that is derived from CI to the context of SNS tracking aiming to provide insight and deeper understanding of the issue.

We will first highlight the outcome of our experiments in Section 2, then look at some key characteristics of Nissenbaum’s CI as well as briefly describe her decision heuristic in Section 3. We then apply the decision heuristic to the experiments’ findings in Section 4 and conclude in Section 5. In addition, we provide a summary of the analysis of our study in Table 5.

2 Wireshark experiments

In 2012, we conducted Wireshark experiments by capturing and analysing the HTTP traffic of the first author’s online browsing activities. We aimed to identify the pieces of user’s information being shared or leaked from first party to third party sites, without user’s awareness or intention to share. First party sites are sites that are directly requested by users while third party sites are not directly connected to by users. Those third party sites can be advertisers or purely data aggregators.

HTTP or HyperText Transfer Protocol is a stateless protocol that is used in communication between the browser or any intermediate devices, and the web servers [Comer(2000)] [Kristol(2001)]. HTTP uses a small text file called an HTTP cookie in order to remember the state of each HTTP request and response. HTTP cookie is stored by browser at user’s machine [Kristol(2001)] and is not intended to be used as a spying mechanism; rather for the purpose of informing the web server that the same user or device has returned [Hormozi(2005)]. However, HTTP cookies can be used by marketers and web
developers to collect users’ information and to track users’ visits and browsing habits. Wireshark is a network protocol analyser that captures and displays all HTTP traffic among the network communication using HTTP protocol, for example, the communication between the browser or application and the requested sites or servers (Figure 1).

2.1 Methods and data collection

The study included performing a set of most common browsing activities based on a survey by Pew Internet [Purcell(2011)] and browsing a set of sites associated with those chosen online activities based on the ranking by Alexa (www.alexa.com). We relied on the data provided by Google statistics for the frequently searched terms for online searches. Table 1 summarised the activities and the associated sites chosen in our experiments.

Each experiment involved the first author performing a set of browsing activities among the selected sites while having her activities recorded by Wireshark. A set of browsing activities included checking and sending e-mails, using SNS while playing Farmville third party application on Facebook, purchasing skin care products (facial masks) on ebay, reading online news articles and searching for fish curry recipe via Google search engine. Each browsing session is saved in different Wireshark files (Figure 1). We then analysed those files by looking at the HTTP headers and reported on the types of information being shared and to whom.
Table 1  Online activities and sites chosen in the experiment

<table>
<thead>
<tr>
<th>E-mail</th>
<th>SNSs</th>
<th>Online shop</th>
<th>Online news</th>
<th>Google search</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo</td>
<td>Facebook eBay 9 MSN News Taste.com.au</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gmail</td>
<td>Twitter LinkedIn Google Plus</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.2 Summary of the findings

2.2.1 Third party sites

Within just one browsing session of the selected sites and activities, first party or visited sites are seen to connect to numerous third party sites (highlighted in Table 2). In addition, as shown in Table 4, first party sites were seen to leak or share user’s identifiable and non-identifiable information to various third party sites. Those third party sites, who are able to acquire users’ information and online movements, were identified to be *advertisers or data aggregators* (e.g. Doubleclick, b.scorecardresearch, imrworldwide) and *SNSs* (e.g. Facebook, Twitter and Google Plus).

Table 2  List of third party sites

<table>
<thead>
<tr>
<th>(1) Taste.com.au</th>
<th>(2) LinkedIn (Farmville application and ads)</th>
<th>(3) Facebook</th>
<th>(4) Facebook (No ads or apps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>news-statistic.com</td>
<td>google-analytics.com</td>
<td>akamaihd.net</td>
<td>None</td>
</tr>
<tr>
<td>sops.news.com.au</td>
<td>imrworldwide.com</td>
<td>googletagservices.com</td>
<td></td>
</tr>
<tr>
<td>trakr-news.com.au</td>
<td>quantserv.com</td>
<td>quantserve.com</td>
<td></td>
</tr>
<tr>
<td>google-analytics.com</td>
<td>b.scorecardresearch.com</td>
<td>b.scorecardresearch.com</td>
<td></td>
</tr>
<tr>
<td>notebookmagazin.com</td>
<td>doubleclick.net</td>
<td>doubleclick.net</td>
<td></td>
</tr>
<tr>
<td>fashion.vogue.com.au</td>
<td>googleadservices.com</td>
<td>googleadservices.com</td>
<td></td>
</tr>
<tr>
<td>doubleclick.net</td>
<td>sunbeamfoods.com.au</td>
<td>rtbidder.net</td>
<td></td>
</tr>
<tr>
<td>trakr-news.com.au</td>
<td>doubleclick.net</td>
<td>socialvi.be</td>
<td></td>
</tr>
<tr>
<td>news-statistic.com</td>
<td>quantserve.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>google-analytics.com</td>
<td>b.scorecardresearch.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>notebookmagazin.com</td>
<td>doubleclick.net</td>
<td></td>
<td></td>
</tr>
<tr>
<td>doubleclick.net</td>
<td>googleadservices.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sunbeamfoods.com.au</td>
<td>rtbidder.net</td>
<td></td>
<td></td>
</tr>
<tr>
<td>doubleclick.net</td>
<td>socialvi.be</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.2.2 The types of shared information

SNSs are seen to leak user’s identifiable information while non-SNSs are seen to share user’s non-identifiable information to third party sites. For instance, LinkedIn leaked user’s identifiable information (name and her unique identifier to LinkedIn [every SNS user is assigned with unique identifier in SNS database]) to third party sites (Table 2, Column 2) including doubleclick as illustrated in Table 3 Row 1. As shown in Table 2 Column 3 and Table 2 Column 4, Facebook is seen to connect to third party sites and share user’s information only when user clicks on advertisements or third party application. Twitter, on the other hand, is seen to share user’s clickstream to third party sites.

Meanwhile, non-SNS like taste.com.au shared user’s search term and clickstream (e.g. fish curry) to various third party sites including SNSs like Facebook while retrieving Facebook’s Like button, as illustrated in Table 3 Row 2. Similarly, Yahoo mail also shared user’s clickstream within Yahoo to advertisers, while Gmail traffic is encrypted in other protocol rather than HTTP and is not observable. Wikipedia, non-profit organisation, is not seen to share any user’s information to other parties.

Table 3 Sample of HTTP headers

<table>
<thead>
<tr>
<th>(1) LinkedIn and doubleclick</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /b? ...</td>
</tr>
<tr>
<td>Host: ad.au.doubleclick.net</td>
</tr>
<tr>
<td>User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:8.0.1) Firefox/8.0.1</td>
</tr>
<tr>
<td>Referer: <a href="http://www.linkedin.com/profile/">http://www.linkedin.com/profile/</a>... a user’s LinkedIn ID and full name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(2) Taste.com.au and Facebook</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET /plugins/like.php? ... User’s Facebook unique identifier</td>
</tr>
<tr>
<td>Host: <a href="http://www.facebook.com">www.facebook.com</a></td>
</tr>
<tr>
<td>User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:20.0) Firefox/20.0</td>
</tr>
</tbody>
</table>

In addition to identifying the shared information and the third party sites, as summarised in Table 4, we also discovered that SNSs such as Facebook, Google Plus and Twitter have the ability to track users’ online movements not only within SNS but also beyond SNS, because the visited sites embedded SNS widgets such as Facebook’s Like button, Google’s Plus One button and Twitter’s Tweet button. For example, Taste.com.au is seen to connect to these three SNSs (Table 2 Column1) in order to retrieve the widgets to display on the recipe page while also sharing user’s searched or viewed recipe (Table 3 Row 2). Those SNS widgets enable users to share content from various websites with their SNS friends by just one click, and also enable site owners to have a view of the number of visits on their domain both daily and demographically [Facebook(2011)] [Twitter(2011)] [Google(2011)]. Moreover, due to this
tracking, SNSs are able to provide more personalised advertisements to their users.

Table 4 The types of shared information and third party sites

<table>
<thead>
<tr>
<th>First party sites</th>
<th>The shared information</th>
<th>Third party sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yahoo</td>
<td>User’s clickstream within Yahoo mail</td>
<td>Advertisers</td>
</tr>
<tr>
<td>Gmail</td>
<td>Encrypted</td>
<td>Encrypted</td>
</tr>
<tr>
<td>Google Plus</td>
<td>Encrypted</td>
<td>Encrypted</td>
</tr>
<tr>
<td>Facebook (No ads or apps)</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Facebook (Ads and apps)</td>
<td>Facebook ID</td>
<td>Advertisers</td>
</tr>
<tr>
<td>Twitter</td>
<td>User’s clickstream within Twitter</td>
<td>Advertisers</td>
</tr>
<tr>
<td>Ebay</td>
<td>User’s searches and clickstream</td>
<td>Advertisers</td>
</tr>
<tr>
<td>9 MSN news</td>
<td>User’s searches and clickstream</td>
<td>Advertisers and SNSs</td>
</tr>
<tr>
<td>Taste.com.au</td>
<td>User’s searches and clickstream</td>
<td>Advertisers and SNSs</td>
</tr>
<tr>
<td>Wikipedia</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

The tracking by SNSs is seen to be problematic because SNSs are already holding or storing large volume of information voluntarily provided by their users, and in addition, they have the ability to acquire information about their users’ online movements. More importantly, SNS users might not be aware that their online activities can be recorded by SNSs. Therefore, this current study will focus on the tracking of online users by SNSs and we would like to find out whether or not this practice impinges on users’ privacy.

3 Contextual Integrity and decision heuristic

3.1 Contextual Integrity

Nissenbaum [Nissenbaum(1997)] [Nissenbaum(1998)] argues that in order to address the challenge in the information technology age, theories of privacy should take into account the information which can be harvested in a public realm. She believes that Privacy in public, which has been ignored in the previous privacy theories, is worthy to be studied and protected in the information age. Nissenbaum [Nissenbaum(1997)] is also opposed to two misleading assumptions: (1) there is a realm of public information about persons to which no privacy norms apply, and (2) an aggregation of information does not violate privacy if its parts, taken individually, do not.

Regarding the first assumption, she argues that public space (e.g. public park or sidewalk) are governed by some norms of privacy and that information collected from those spaces is not completely public. For example, when asked for their name by a complete stranger in the public park, an individual is entitled to answer “None of your business ”. Moreover, she also points out that an individual has a right in controlling the dissemination of personal information even if it happened in a public area. For instance, even though
a rape case occurred in a public park, the rape victim as well as her family retain some measure of control over the information about them - particularly her identity.

In response to the second assumption, she indicates that collecting, compiling, and combining innocuous bits of information of an individual can be invasive of his/her privacy because those bits of information can reveal a rich portrait of that person. Technology has enabled us to collect large amounts of information in a short period of time and to draw meaningful inferences from them which can be embarrassing to an individual. She also adds that the act of compiling information which involves moving information across different contexts results in information being used in a manner that is not explicitly known when it was initially collected. Therefore, this act failed to get permission from users to move their information around.

Seeing that previous philosophical and legal theories of privacy offered limited justification for dealing with the problem of privacy in public, Nissenbaum introduced Contextual Integrity (CI) as a privacy benchmark [Nissenbaum(2004)]. CI focuses on the notion of a context to analyse whether or not a flow of information, either gathering or dissemination, is appropriate with the norms within a context. Contexts refer to “structured social settings with characteristics that have evolved over time (sometimes long period of time) and are subject to a host of causes and contingencies of purpose, place, culture, historical accident, and more” [Nissenbaum(2010)].

Almost everything we do including acting, and interacting with others, takes place in contexts (e.g. education, health care, employment, family, business, and religion). People also navigate across different contexts through out the day [Nissenbaum(2010)]. For example, Jane Doe is a PhD candidate at Charles Sturt University. She is also working as a part time web developer for a private organisation. She spends time watching television with her family, goes to her office on a daily basis, goes to work every Tuesday and Thursday afternoon, goes shopping, seeks medical care every six months, and goes to concerts with her friends.

Each context is also characterised by different roles, is partly constituted by canonical activities that are oriented around values, and is governed by behaviour-guiding norms that prescribe and proscribe acceptable actions and practices [Nissenbaum(2010)]. For example, in the context of education, Jane’s role is a PhD candidate or student at the School of Computing and Mathematics at Charles Sturt University where some of her activities include conducting interviews for her research, analysing the data and writing up the reports. The value of the education or her role as a PhD candidate is to create new knowledge and contribute to the literature. The norms prescribe that Jane as well as other PhD candidates submit progress reports to the Research Office every six months.

Norms also define duties, prerogatives, obligation, and privileges of roles, as well as acceptable and unacceptable behaviours [Nissenbaum(2010)]. Among the norms present in most contexts are those that govern the flow of information about people in the contexts. Contextual Integrity prescribes two types
of information norms: (a) norms of appropriateness, and (b) norms of distribution.

Norms of appropriateness circumscribe the type of information about an individual that is appropriate, expected or allowable to be revealed in a particular context. For example, in the context of education, it is appropriate that the Research Office at Jane’s university know her PhD progress, but it is not appropriate that they also know her medical condition details.

Norms of distribution, on the other hand, govern the flow or distribution or dissemination of information from one party to another. For instance, within a health care context, it is appropriate that Jane’s General Practitioner (GP) access her medical records, and divulge those details with other GPs or specialists if needed, but it is not appropriate that he provide these details to Jane’s employer.

Contextual Integrity of the information flow is maintained when both norms are respected, otherwise, a violation of privacy occurs.

3.2 Decision heuristic

Despite the claim that contextual integrity has been proposed as a justificatory framework for evaluating new technology-based systems and practices which affect the flow of information in moral and political terms, there is a potential criticism which goes against the framework. The critics argue that the framework is conservative, hence, is not easily adaptable to new technologies where there are no pre-existing expectations or norms governing the flow of information [Nissenbaum(2010)]. Nissenbaum addresses the concern by responding with a decision heuristic derived from the framework and augmented by some prescriptive elements, which she notes will help explain the source of the problem and evaluate systems or practices in question. Her decision heuristic nine steps, in brief, include (more details on these in Section 4):

1. Describe the new practice in terms of information flows
2. Identify the prevailing context ...
3. Identify information subjects, senders, and recipients.
4. Identify transmission principles.
5. Locate applicable entrenched informational norms and identify significant points of departure.
6. Prima facie assessment ...
7. Evaluation I ...
8. Evaluation II ...
9. On the basis of these findings, contextual integrity recommends in favour of or against the systems or practices under study ... [Nissenbaum(2010), p. 181-183]

Nissenbaum mentions that the decision heuristic is applicable in addressing privacy online which should be done in the same way as when we analyse privacy in general because our online activities are deeply integrated into our
social life. For example, banking transaction, previously rooted in our offline routine can now be done online. In order to address privacy online, one needs to locate context, explicate informational norms, identify the disruptive flows of information and evaluate those flows against norms based on general and political principles as well as context specific purposes and values.

She emphasises that locating context online and explicating the norms can be done easily for some activities which are similar to offline activities - like in the context of banking, either we make a bank transaction over the phone, or face-to-face with a bank teller, or online, there is a common expectation that the transaction should be done in a confidential and secure manner. On the other hand, locating context and norms of online activities, which do not have comparable activities in our offline life, can be challenging. For instance, it can be hard to locate the context and norms of an online search engine because it might not have obvious counterparts in real life.

Consequently, Nissenbaum [Nissenbaum(2011)] provides two other broad recommendations on top of the decision heuristic in order to help in locating the context and norms among online cases that do not have clear social precedents. First, we should look for the similarities of that online case or activity to the social activity and structure. The norms or restraints on the flow of information can be drawn out from those similarities. Second, without having to look for the similarity of that online activity to an offline one, we can work out the norms by looking at the ends, purposes and values of the site or organisation. For instance, unlike the context of banking, a search engine does not hold a clear social precedent. If consulting a search engine can be seen as analogous to conducting research and seeking information in a library catalogue, then the norms would be strict confidentiality with regard to the search histories as practiced by many libraries.

4 Applying decision heuristic to the SNS tracking

Step 1: Describing the new practice in terms of information flows

SNS users provide SNSs with their information in order to sign-up for an SNS account, and later, generate other contents on SNSs in order to interact with other people. SNSs are seen to be already holding large volumes of information provided by users. On top of that, they also have the ability to track user’s movements within and outside SNSs, particularly among websites that use SNS widgets (e.g. Facebook’s Like button, Twitter’s Tweet button, and Google’s Plus one button). They are also seen to disseminate users’ information to various third party sites (e.g. Facebook transfers users’ information to Farmville application, and Twitter shares user’s clickstream to third party sites).
Step 2: Identify the prevailing context

This step requires that we establish context at a familiar level of generality like health care or education. Unlike the context of an online bookstore, online pharmacy or online banking, SNS is a unique phenomena that does not hold a clear social precedent; hence it is challenging to locate the context and explicate the norms [Nissenbaum(2011)]. For this particularly online activity, it is suggested that we look at the similarities of SNS structure to the social activity [Nissenbaum(2011)].

Looking at SNS structure, we observe that SNS consists of multiple profiles. Each profile comprises of several features such as profile information, wall post, album pictures, private message, and advertisement banners. Every post of activity on SNS profiles are recorded and are retrievable. The notion of a community in real life appears to be a useful term given an SNS community has private spaces (profiles) like houses in a real community. A community in real life refers to “(1) a group of people (2) who share social interaction (3) and some common ties between themselves and the other members of the group (4)… who share an an area [physical space] for at least some of the time...” [Al-Saggaf(2004), p. 2]. Meanwhile, boyd and Ellison [boyd and Ellison(2007), p. 211] define SNSs as “web-based services that allow individual to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”. boyd and Ellison [boyd and Ellison(2007), p. 211] also add that what makes SNSs unique is that SNSs enable users to articulate their social networks with people who share some offline connection with them. The above definition of a community shares most of the aspects as presented in the definition of an SNS above; hence, an SNS is seen to serve as a platform on which a community exists.

Let us compare an SNS to a real life community and an SNS profile to a house in a community. The process of one signing up for an SNS account and getting an SNS profile is similar to a process of one buying a house within a community. Each house comprises of several features and rooms or sections; for example, a living room area where the owner can hang out and interact with her friends, or her friends can leave her notes at the door when she is not present in the house, photo albums, and a mailbox where one can drop her a letter. Having one’s SNS profile private is similar to a user using an access card to lock up the house to limit access from the public or random people. A public profile is like an unlocked house where anyone can just walk in. If the community owner provides different levels of privacy setting, the user has the ability to provide a different level of access to the house to different people they befriend.
Step 3: Identify information subjects, senders and recipients

The agents, senders and recipients, refer to those from whom and to whom the information flows, and information subject refers to the one whom the information is about [Barth et al(2006)Barth, Datta, Mitchelle, and Nissenbaum]. Based on the findings of our study, SNSs (Facebook, Twitter, and Google Plus), users and third party sites are the main agents. Users, as senders, provide or send personal information about them to SNSs to populate their SNS profiles and interact with other SNS users. SNSs, as recipients, collect, receive and store information about users (information subject) such as personal information and information about their browsing habits. SNSs, as senders, transfer or leak users’ information to third party sites, as recipients.

Step 4: Identify transmission principles

A transmission principle refer to the constraints on the flow of the information from party to party in a context in terms of the distribution, dissemination, and transmission of the information. This should detail the terms and conditions related to the appropriateness of the information flow [Barth et al(2006)Barth, Datta, Mitchelle, and Nissenbaum], [Nissenbaum(2010)]. We examined privacy policies of Facebook [Facebook(2012a)], Twitter [Twitter(2012)], and Google Plus [Google(2012)] to find out what they say about the information collection and distribution. Basically, SNS collect any information provided and generated by their users as well as their movements or activities within SNS, including the information provided upon the registration and the information populated in one’s profile page. The policies also state that SNSs collect information about users whenever users visit websites or applications that use SNS platforms or widgets. In addition, SNSs also share information, both personal and non personal information about users to other parties (such as their service providers) and other users within the system.

Step 5: Locate applicable entrenched informational norms and identify significant points of departure

The framework suggests that we identify the established informational norms and the significant changes brought by the practice under study. SNSs are now able to collect not only personal information about their users, but also about their movements and activities within and outside the SNS boundary. An SNS widget (e.g. a Facebook’s Like button, or a Twitter’s Tweet button, or a Google Plus’s Plus One button) resembles a CCTV camera within and outside a community. How a CCTV camera is setup can be questionable and should be investigated further as to whether or not there is a breach of privacy or entrenched norms. So now the question is did SNSs acquire informed consent from their users regarding the set-up of the CCTV camera, or the collection and dissemination of users’ information?
By looking at SNS privacy policies [Facebook(2012a)] [Twitter(2012)] [Google(2012)], and if we rely on these policies as transmission principles, it appears ostensibly that they conform to what they state in the policies regarding what they collect or disseminate and how. The transmission principles also allow for commercial exchange of information in accordance with the rules of a competitive free market, but it requires the sender’s knowledge (or notice), and/or permission (consent) [Nissenbaum(2010), p. 145].

However, Barocas and Nissenbaum point out how privacy policies, the approach of notice-and-consent or informed consent, have not proved to be successful approaches to addressing privacy online [Barocas and Nissenbaum(2009)] [Nissenbaum(2011)]. For one reason, if we want all details about the data collection and distribution, privacy policies will be too long, and if they are too short, they may as well miss out all the details [Nissenbaum(2011)]. For example, Google’s privacy policy alone accounts for approximately 2500 words, excluding the sub links or sub pages of the policy [Google(2012)]. The other reason is that the policies are constantly changing [Barocas and Nissenbaum(2009)] [Nissenbaum(2011)]. Twitter already has five versions of the privacy policies since it was launched in 2006 [Twitter(2013)]. We also examined the archives of the available policies (Twitter and Google). There are changes regarding the information collection. For example, only in the new policy [Twitter(2012)] does Twitter address the information collection via the Tweet button.

In addition, users also have difficulties in achieving meaningful understanding of the practices (information collection and distribution) to which they are expected to be able to consent [Barocas and Nissenbaum(2009)]. For example, users need to have basic knowledge in technologies or business in order to understand what HTTP cookies or third parties are, and in order to fully understand the following part of privacy policy:

“...We receive data whenever you visit a game, application, or website that uses Facebook Platform or visit a site with a Facebook feature (such as a social plugin), sometimes through cookies... Sometimes we get data from our affiliates or our advertising partners, customers and other third parties that helps us (or them) deliver ads... [Facebook(2012a)] ”,

Moreover, language barrier is another obstacle faced by many users whose English is not their mother-tongue. For instance, Facebook’s and Twitter’s privacy policies are available only in English language, although recently, Facebook makes Khmer language (the official language used in Cambodia) available on their site (Cambodia is the first author’s home country). On the other hand, Google’s privacy policy is available in many languages except in Khmer.

In terms of choice, SNSs give users two options: either to agree with all the listed terms and conditions and sign up for an account or to not be able to use SNS services at all. For Facebook and Twitter, by clicking on the sign up button, it automatically means that the users agree to the terms and conditions. For Google, without ticking on the check-box of agreement, the sign up will not proceed. Users who previously signed up for an SNS account might agree to the terms and conditions at the time of signing up, but they may not agree to the recent tracking and targeting. Facebook, Twitter and Google do send
out notifications to their users regarding the changes in their policies. But are users allowed or able to opt-out from the new policies or practices? Or while they already provided and generated large amounts of information to SNSs, and connected with many other users, should they remove themselves from SNSs completely when they are not happy with the changes to the policies?

According to Barocas and Nissenbaum [Barocas and Nissenbaum(2009), p. 5], in order for users to make an informed choice and consent, they must understand “(1) Which actors have access; (2) What information they have access to; (3) What they do or may do with this information; (4) Whether the information remains with the publisher or is directly or indirectly conveyed to third parties; and (5) What privacy policies apply to the publisher as compared to all the third parties, assuming these are even known to the users...”. SNSs did not make it obvious who their affiliates or advertising partners are, so users do not have access to privacy policies of those third parties regarding the use of their information. In addition, because of the length and fickleness of privacy policies, jargons and language barriers within the policy contents, we assume that SNS users do not fully understand or are not aware of (1) who the stakeholders are, (2) what information about them is gathered by SNSs and third parties, (3) how their information will be used, (4) whether their information remains with SNSs or shared to third parties, and (5) what policies apply to SNSs, third party sites, as well as any websites they visited or wish to visit. Therefore, Facebook, Twitter and Google Plus did not gain informed or active consent from their users in moving their information across different contexts and in tracking their users’ online movements. To be able to give informed consent, users are expected to read carefully to fully understand privacy policies of websites they intend to visit.

If we rely solely on SNSs’ privacy policies to define the norms in the information flows within SNS contexts, it appears to us that SNSs conform to what they state in their policies regarding the collection and dissemination of users’ information. However, based on the arguments and rationales regarding the inadequacy of privacy policies, it appears to us users are not explicitly informed about the tracking by SNS widgets and SNSs did not gain their informed consent in setting up and using these widgets. The departure from the entrenched practice in this context is the SNS widget (Facebook’s, Twitter’s, or Google’s widget) that resembles hidden CCTV camera used to capture users’ movements within and outside a community. Prior to the existence of the widgets, SNSs can only record users’ activities within SNS boundaries.

Step 6: Prima facie assessment

Within this step, a decision can be made as to whether or not the practice under study violates the information norms. By going through Step 1 to 5 of the decision heuristic and by examining privacy policies among SNSs (Facebook, Twitter, and Google Plus), we argue that SNSs did not gain informed consent from their users regarding the collection and distribution of their in-
formation. SNS widgets are seen to be hidden CCTV cameras that are used to record users’ movement within and outside the community. The descriptive component of the heuristic establishes that such tracking constitutes a breach of information norms, and consequently a violation of contextual integrity. However, further steps assessing the legitimacy of the tracking are required by the heuristic.

Step 7: Evaluation I

The framework also suggests that we consider the moral factors affected by the practice in terms of harms and threats to autonomy and freedom. Regarding the privacy policies as transmission principles, Facebook, Twitter and Google Plus did not gain informed consent from their users in recording their online movements across different sites and in moving their information across different contexts. Users are not aware of the tracking or recording; hence, they have the impression that their online activities are private.

On the bright side, the tracking allows SNSs to provide relevant advertising contents to their users. The ads are usually based on their users’ browsing preferences or habits. For example, by visiting a recipe web site like Taste.com.au, the theme of cooking can be drawn from this browsing; the useful advertisements for the users could be sales or bargains related to kitchen utensils or cookbooks.

On the other hand, the tracking or the recording by the hidden camera seems to be doing something wrong and affecting one’s autonomy. Personal autonomy is one of the four functions of privacy that Westin [Westin(1966)] refers to as “the desire to avoid being manipulated or dominated wholly by others.” Westin argued that privacy protects autonomy in terms of individuality and consciousness of individual choice in life. He also added that another aspect of autonomy is the individual’s sense of he who decides when to “go public”. In this case, SNS users are being observed and their browsing activities within and across different sites can be recorded by the SNS (Facebook, Twitter and Google Plus). Therefore, online users’ autonomy is deteriorated to some extent.

Without the fear of being observed, or judged by others and without the constraints and expectation of a convention, an individual has more freedom to formulate life choices, preferences and commitment for themselves [Nissenbaum(2004)]. The context of SNS tracking without users being well-informed impinges on the users’ freedom to some degree. Users’ choices of browsing activities could be different if they are aware of the tracking or monitoring. In this case, little do they know that the SNS widgets can serve as a CCTV camera, nor are they well informed about the monitoring. They could be more cautious and selective with some visits to specific sites if they know their activities are recorded by SNS.

To sum, users thought they had complete freedom and autonomy regarding their browsing activities, and presumably, they thought their online activities
were in a private zone, when in fact SNSs are able to know what they are doing online.

Step 8: Evaluation II

In addition to considering the impact on autonomy and freedom, the framework also suggests that we consider if the practice also impinges on the values, goals, and ends of the context.

The central goal or value of an SNS is to provide a means of communication between people where they can connect with each other [boyd and Ellison(2007)]. The goal and mission of Facebook is to make the world more open and connected by giving people the power to share [Facebook(2012b)]. Facebook is seen to enjoy a tremendous success while attracting a billion active users in mid 2012 owing to the fact that they succeed in delivering such a communication service expected by their users.

SNS users are usually allowed to set their profiles to a private mode, where they can allow visibility to a limited audience. However, the notion of “private profile” gives users the wrong impression that only their limited audience would see what they share because most users have no clue that their information and browsing activities are being shared to third party sites, and tracked by SNSs in the HTTP headers.

Facebook, Twitter and Google Plus do deliver the expected communication services based on their goals and mission. However, the SNS tracking appears to go beyond their mission as well as users’ expectations of connecting and communicating with their friends. Within the context of SNS or community, users expect to be able to share experiences and communicate with other users, but not to be tracked and monitored across different sites. Privacy policies which are frequently changing, and long, fail to formally inform the users about the tracking. Therefore, the users think or expect that their online activities are private, but actually they are not.

Step 9: Recommendation

This is the step where the framework recommends in favour of or against the practice under study on the basis of the findings in the previous eight steps [Nissenbaum(2010)].

Earlier, we provided an analogy of a community to an SNS in order to locate the entrenched norms. We also examined privacy policies among Facebook, Twitter, and Google Plus only to find out that SNS already listed all the terms and conditions of this current practice (data collection via the use of SNS widgets). However, after examining the approach to online privacy by using privacy policies and its inadequacy, we argued that SNSs fail to gain informed consent from their users in collecting and disseminating their information. Hence, SNS widgets can be compared to hidden CCTV cameras used to capture and monitor users’ movement within and outside the community.
In step 7 we argued that the user’s autonomy and freedom are being im-
pinged due to the fact that the users are not formally or explicitly informed
about the monitoring, therefore, they assume what they are browsing is pri-
vate when in actual fact it is not. Meanwhile, in step 8, we also argued that
the practice also impinges on the context’s goals, values and ends owing to the
fact that within an SNS or a community context, users have an expectation
of being able to connect and communicate with other users, but they might
not expect that their online activities across non-SNS sites can be monitored
by the SNS.

Does the tracking by SNSs really improve the SNS users’ experience? Prior
to the availability of the SNS widgets, users simply copied a specific URL of a
page and pasted in their profile page in order to share that link to their SNS
friends. SNSs were able to know what users do only within SNSs. What SNS
widgets enable is a single click (either on Facebook’s Like button, or Twitter’s
Tweet button, or Google’s Plus One button) for users to share things on their
profiles.

On one hand, the SNS widgets improve the users’ experiences in sharing
their preferences while also enabling the SNSs to track their users’ movements
across different sites that embedded those widgets; therefore, enabling SNSs
to provide a better targeted advertisements to the users. On the other hand,
with the absence of SNS widgets, users still can do the sharing, and the CCTV
cameras are not present. The advertisements are still there except they are not
as personalised as when the widgets are present.

We also examined privacy settings among Facebook, Twitter, and Google
Plus. Currently, Facebook and Twitter provide users the ability to manage the
widgets. Managing Facebook’s widget means users have the choice to whether
or not display the pages they “Liked” on their profiles or newsfeed, as shown
in Figure 2. Meanwhile, disabling Twitter’s widget means “Stop Twitter from
tailoring Twitter based on my recent website visits”. Google Plus does not
provide users option to disable or enable their widget. Nonetheless, managing
Facebook or Twitter’s widget only limits the visibility of tailored advertise-
ments or Tweets and browsing activities from users and their friends, but does
not stop Facebook and Twitter from tracking online movements, because their
widgets are still present after they were disabled via Facebook’s and Twitter’s
privacy setting.

Therefore, based on our rationale and argument so far, we recommend that
the framework reject the practice of tracking and monitoring SNS users by
SNS companies (like Facebook, Twitter, and Google) across non-SNS. Within
an SNS context, it is appropriate that SNS collects users’ information within
SNS boundary for the purpose of improving users’ experiences in connecting
with other users, and for the purpose of improving SNS services in terms of
efficiency in troubleshooting and analysis of the site performance or network
traffic. But it is not appropriate that SNS also collects information about
their users’ online movement outside SNS boundary, and disseminates their
information to other parties without users being explicitly informed.
Contextual Integrity’s decision heuristic and social network sites tracking

Fig. 2 Managing Facebook’s widget

5 Conclusion

Contextual integrity, introduced by Helen Nissenbaum, is intended as a framework to account for people’s reaction to a technology or system that affects the information flows, as well as a tool to evaluate the practice of a technology or a system from a moral and political view point. The framework focuses on a context and the flow of the information, rather than the types of information. It also argues for protection of information in the public space and any non-sensitive information divulged in a specific context. The fact that the information is infused or available in public or the information is non-personal or non-sensitive does not mean it can be up for grabs.

In addition, Nissenbaum also developed a decision heuristic (derived from contextual integrity) which helps to respond to privacy challenges posed by new emerging technologies like SNS. The decision heuristic suggests that we locate contexts, explicate the informational norms, identify the disruptive flows of information, and evaluate the flows against the norms based on general moral and political principles as well as context purposes, ends, and values.

This article focuses on the application of Nissenbaum’s decision heuristic to our findings that revealed that SNS, particularly Facebook, Twitter and Google Plus, are able to track the users’ browsing activities not only within the SNS themselves but also outside the SNS, particularly among web sites that embedded SNS widgets (e.g. Facebook’s Like Button, Twitter’s Tweet Button, and Google’s Plus One button). SNSs are also seen to share users’ information to third party sites who appear to be their advertising partners. We analysed the situation by comparing a real life community to an SNS
and by going through the nine steps of the decision heuristic (summarised in Table 5). We also examined the privacy policies of Facebook, Twitter, and Google Plus.

Steps 1 to 4 of the heuristic introduced us to what the practice is, who the stakeholders are, what the context is and what the transmission principles are. Users, SNSs and third party sites are the main agents or stakeholders while users’ information flow across different contexts among first party and third party sites. In step 5 of the heuristic, we discovered that there was a breach of the informational norm from the practice under this study when SNSs fail to gain informed consent from their users because of the weaknesses of privacy policies. Therefore, SNS widgets are seen to be analogous to hidden CCTV cameras used to record and monitor the residents’ movements within and outside the community.

In steps 7 and 8, we argued that the users’ autonomy and freedom are being threatened because they are not explicitly informed about the tracking, and the tracking also impinges on the goals, values and ends of an SNS or a community where users expect to be connected with the other people, but not to be tracked and monitored by SNS. Meanwhile, in the 9th step of the heuristic, we propose that the practice we studied is rejected by the framework because SNS users’ right to privacy is being violated by the practice of SNS tracking across non-SNS sites.

However, we live in a society where technologies are evolving and always moving forward. There should be a trade off or a balance of benefits of the widgets to both users and SNSs. [Hull et al(2011)Hull, Lipford, and Latulipe] mentioned that the design of a system, in their case Facebook’s News Feed feature, that may raise privacy issues can be addressed through a better design so that information flow can be more transparent to users. Likewise, the practice of using SNS widgets (Like button, Plus One button, and Tween button), which leads to the tracking of users’ movement across sites, can be favoured or accepted by the CI framework if there is a change in the design in which SNSs give users choice or freedom to enable or disable the widgets (or hidden camera) completely. Or at least, the design should make the tracking explicitly clear to users so that they are well-informed about such a practice and are able to make better decisions with regards to SNS usage.

References

Contextual Integrity’s decision heuristic and social network sites tracking


[Facebook(2012a)] Facebook (2012a) Data use policy. URL http://www.facebook.com/about/privacy/

[Facebook(2012b)] Facebook (2012b) Facebook: about. URL http://www.facebook.com/facebook/info


[Twitter(2011)] Twitter (2011) Twitter buttons. URL http://twitter.com/about/resources/buttons


[Twitter(2013)] Twitter (2013) Previous twitter privacy policies. URL http://twitter.com/privacy/previous

### Table 5 Decision heuristic and the practice under study

<table>
<thead>
<tr>
<th>Step</th>
<th>Description of the new practice</th>
<th>The practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Step 1: Description of the new practice</td>
<td>Facebook, Twitter and Google Plus are able to not only collect and analyse users’ information but also track users’ movement across sites which embedded Facebook’s Like Button, Twitter’s Tweet button and Google’s Plus One button</td>
</tr>
<tr>
<td>2</td>
<td>Step 2: Prevailing context</td>
<td>We provided an analogy of an SNS to a community in real life</td>
</tr>
<tr>
<td>3</td>
<td>Step 3: Information subjects, senders and recipients</td>
<td>Users: Senders and information subjects, SNSs: senders and recipients of users’ information, Third party sites: recipients of users’ information from SNSs as recipients</td>
</tr>
<tr>
<td>5</td>
<td>Step 5: Informational norms and significant points of departure</td>
<td>Because of the weaknesses of privacy policy approach to online privacy, SNSs did not gain informed or active consents from their users in tracking their movements across different sites, and in moving their information across different contexts SNS failed to conform with the transmission principle of notice and consent by not having a transparent notice and permission from their users. Therefore, an SNS widget serves a role as a hidden CCTV camera.</td>
</tr>
<tr>
<td>6</td>
<td>Step 6: Prima facie assessment</td>
<td>The descriptive component of the heuristic establishes that such tracking constitute a breach of information norms, and a violation of contextual integrity</td>
</tr>
<tr>
<td>7</td>
<td>Step 7: Evaluation I (harms and threats to users’ autonomy and freedom)</td>
<td>Users’ autonomy and freedom are impinged: they thought they have complete freedom and autonomy upon their browsing activities and they thought their online activities are in a private zone while actually they are being monitored by SNS.</td>
</tr>
<tr>
<td>8</td>
<td>Step 8: Evaluation II (values, goals and ends of the context)</td>
<td>SNS tracking appears to be beyond SNS mission as well as users’ expectation of connecting and communicating with friends. Privacy policies are changing, too long, and fail to formally inform users about the tracking</td>
</tr>
<tr>
<td>9</td>
<td>Step 9: Recommendation</td>
<td>The framework rejects the practice of tracking and monitoring of users by SNS companies across non-SNS sites unless users are given choice to opt out, or unless users are well informed about the practice.</td>
</tr>
</tbody>
</table>