Information Systems Research

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook

Huseyin Cavusoglu, Tuan Q. Phan, Hasan Cavusoglu, Edoardo M. Airoldi

To cite this article:
Huseyin Cavusoglu, Tuan Q. Phan, Hasan Cavusoglu, Edoardo M. Airoldi (2016) Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook. Information Systems Research 27(4):848-879. https://doi.org/10.1287/isre.2016.0672

Information Systems Research
Vol. 27, No. 4, December 2016, pp. 848–879
ISSN 1047-7047 (print) | ISSN 1526-5536 (online)

https://doi.org/10.1287/isre.2016.0672

Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook

Huseyin Cavusoglu
Naveen Jindal School of Management, University of Texas at Dallas, Richardson, Texas 75083, huseyin@utdallas.edu

Tuan Q. Phan
School of Computing, National University of Singapore, Singapore 117418, tphan@comp.nus.edu.sg

Hasan Cavusoglu
Sauder School of Business, University of British Columbia, Vancouver, British Columbia V6T 1Z2, Canada, cavusoglu@sauder.ubc.ca

Edoardo M. Airoldi
Department of Statistics, Harvard University, Cambridge, Massachusetts 02138, airoldi@fas.harvard.edu

We examine the role of granular privacy controls on dynamic content-sharing activities and disclosure patterns of Facebook users based on the exogenous policy change in December 2009. Using a unique panel data set, we first conduct regression discontinuity analyses to verify a discontinuous jump in context generation activities and disclosure patterns around the time of the policy change. We next estimate unobserved effects models to assess the short-run and long-run effects of the change. Results show that Facebook users, on average, increase use of wall posts and decrease use of private messages after the introduction of granular privacy controls. Also, users' disclosure patterns change to reflect the increased openness in content sharing. These effects are realized immediately and over time. More importantly, we show that user-specific factors play crucial roles in shaping users' varying reactions to the policy change. While more privacy sensitive users (those who do not reveal their gender and/or those who have exclusive disclosure patterns ex ante) share more content openly and less content secretly than before, less privacy sensitive users (those who reveal their gender and/or those who have inclusive disclosure patterns ex ante) share less content openly and more content secretly after the change. Hence, the policy change effectively diminishes variation among Facebook users in terms of content-generation activities and disclosure patterns. Therefore, characterizing the privacy change as a way to foster openness across all user categories does not reveal the change's true influence. Although an average Facebook user seems to favor increased openness, the policy change has different impacts on various groups of users based on their sensitivity to privacy, and this impact is not necessarily toward increased openness. To our knowledge, this is the first study that relies on observational data to assess the impact of a major privacy change on dynamic content-sharing activities and the resulting disclosure patterns of Facebook users.

Keywords: online social networks; privacy; privacy controls; content sharing; disclosure; openness; secrecy
History: Rob Fichman, Ram Gopal, Alok Gupta, Sam Ransbotham, Senior Editors; Ram Gopal, Associate Editor. This paper was received on February 27, 2015, and was with the authors 7 months for 3 revisions. Published online in *Articles in Advance* November 4, 2016.

1. Introduction

Online social network (OSN) platforms, such as Facebook, Twitter, and LinkedIn, are the hallmarks of the Internet. Millions of users from all around the world use these platforms daily to share peer-produced content, including status updates, pictures, videos, comments, tags, and messages, with many other users. Despite the widespread popularity of OSN platforms, privacy remains a thorny issue. Cyberstalking, location revelation, social profiling, divulging sensitive information to third parties, government surveillance, and unintended disclosure are notable examples of the threats to privacy that are exacerbated by OSN platforms.[1] Although many OSN sites have been criticized by privacy groups for a lack of attention to and concern for the privacy of their users (Korth 2012, Electronic Privacy Information Center 2013), these platforms have continued to make inroads into new user bases. Today, OSNs are among the fastest growing and most visited sites on the Internet; Facebook, the largest OSN site, reached 1.55 billion monthly active users in September 2015 (Facebook 2015).

Advertising is the main, and in most cases the only, source of revenue for OSN platforms, as users sign

[1] See http://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_sites.

up for these sites for free.[2] OSN sites can effortlessly gain insights into the lives of users through voluntarily generated content, such as discussions, peer communities, revealed preferences for products and brands, and geolocation content. This unique aspect creates a powerful advertising tool not only in matching people with advertisers but also in spreading the message across the network of friends, thereby facilitating peer influence (Chen et al. 2016). In addition to content production, consumption of peer-produced content through the "captured eyeballs" of friends and other recipients further generates revenue for OSNs via the sale of advertising banners and impressions. However, this opportunity (i.e., the ability to target people) hinges on OSN users creating more content and sharing it openly on the platform and engaging more with others. Therefore, the majority of OSNs have aimed at promoting content generation and openness in sharing content among their users, with an understanding that has long been recognized by social marketers: "Encourage people to be public, increase ad revenue" (Naone 2010). In explaining Facebook's interest in openness, Barry Schnitt, director of corporate communications and public policy, said, "Becoming less private and more public is a change just like it was a change in 2006 when Facebook became more than just people from colleges. Facebook is changing, and so is the world." He also said, "By making the world more open and connected, we're expanding understanding between people. . . . From a business perspective, if users are finding more value from the site, they will come back more and engage in more activity. And you can imagine the business consequences of that" (Kirkpatrick 2009). As Schnitt implied, increased openness (i.e., being more public and less private in sharing content) facilitates not only more traffic to OSN platforms but also more advertising revenues as OSNs can better understand and target their users when the users divulge information about their lives and their favorite things widely, including products, music, movies, and more. OSNs can measure what people are talking about and leverage it for real-time searches, giving advertisers an accurate picture of users' interests and helping them deliver relevant ads to target audiences (Williams 2012).

In this paper, we question the role of privacy changes enacted by OSNs in fostering the openness of information exchange among OSN users. Specifically, we examine the relationship between enhanced privacy controls and disclosure patterns of users based on content-sharing activities in the context of Facebook.[3]

[2] Facebook earned more than 95% of its revenue in the third quarter of 2015 from advertising (Facebook 2015).

[3] We also refer to Facebook as "the OSN platform."

Although Facebook has revamped its privacy policy several times over the years, the changes have mostly dealt with default privacy settings regarding different classes of personal information in user profiles (Freeman 2012). With these policy changes, the OSN platform aimed to make user profiles and generated content widely accessible via permissive settings. Most of these changes have not rolled out new privacy controls per se, but rather redefined the defaults in privacy settings. However, these changes have been heavily criticized by privacy groups as attempts to erode the privacy of OSN users and gradually lower their privacy expectations (Anderson 2010). After studying the changes made by the platform in the past, the Electronic Frontier Foundation concluded, "Viewed together, the successive policies tell a clear story. Facebook originally earned its core base of users by offering them simple and powerful controls over their personal information. As Facebook grew larger and became more important, it could have chosen to maintain or improve those controls. Instead, it's slowly but surely helped itself—and its advertising and business partners—to more and more of its users' information, while limiting the users' options to control their own information" (Opshal 2010).

Limiting access to shared content is a key issue when privacy is concerned. To address the worries of privacy advocates regarding limited controls, the potential backlash of its users, and the possibility of future regulation by the government, Facebook made a major change in its privacy policy in December 2009. On December 9, 2009, the OSN platform announced that it had revamped the tools for privacy to enable its users to better control information they share on the site (Sanghvi 2009). In addition to offering a simple privacy settings page, this change made it possible for users to apply privacy controls to determine access permission at a higher level of granularity than choosing the same audience for each wall post (Cheng 2009). More than 350 million users were asked to review and update their privacy settings. With this major change, Facebook aimed to respond to privacy criticism in a big way by allowing users to control the recipients of content they broadly share. However, the change was heavily criticized by privacy groups because the true intention was seen not as an attempt to give people more control to protect their privacy, but rather to nudge people to share openly even more (Bankston 2009, Kincaid 2009). The OSN platform was thought to be pushing for more openness in content sharing *indirectly*, this time by empowering users with a feeling of control, rather than relaxing default access settings *directly*, as done in the past (Kincaid 2009). Even a Facebook spokesperson implicitly acknowledged this

argument by saying "so long as they [users] feel in control of who sees what, everyone seeing things they post will likely be good for most people" (Kirkpatrick 2009). Furthermore, in explaining the utmost interest of the OSN platform in promoting openness in content sharing through improved privacy controls, Mark Zuckerberg, the chief executive officer (CEO) of Facebook, said, "When people have control over what they share, they want to share more. When people share more, the world becomes more open and connected" (FB News Room 2010). Whether giving users more powerful privacy controls was purely a response of the platform to privacy outcries as it transitioned from a network-based privacy model to a more granular model, or whether this change was intended to bring about more openness in content sharing, is an empirical question.

Since the policy change was purely exogenous to users, it provides a natural experiment setting to study the impact of giving users more control over information they generate and share on the platform. Specifically, we seek to determine whether this change, which introduced granular privacy controls, structurally affected the content-generation/sharing activities and resulted in more accessible disclosures, as supposedly intended by Facebook and anticipated by privacy advocates. Has this change really increased (decreased) the amount of user-generated content shared via wall posts (private messages)? Has this change increased the openness of disclosures?

We focus on the policy change in December 2009 for a number of reasons. First, Facebook added a long-awaited feature to set permissions on a per-post basis. For the first time, Facebook users were able to define the intended audience for each wall post separately, instead of being forced to use the same audience (Sanghvi 2009). Previously, Facebook users had to go with a universal audience selector—everyone, only friends, or friends of friends—for each and every post. With the change, at each posting instance, Facebook users can not only choose a different audience but also customize the audience to a specific group such as individual friends or lists. Second, prior policy changes received limited media coverage. In the early days, most Facebook users might also not have been knowledgeable about privacy threats and the potential implications of these policy changes on their privacy. Hence, it was difficult, if not impossible, to measure the effect of the policy changes and to attribute the resulting impact on users' sharing behavior to them. On the other hand, the change in December 2009 received a considerable amount of publicity. According to Google Trends, Web searches of the terms "privacy," "privacy settings," "OSN privacy," and "privacy Facebook" had a peak search volume of 100 in the category of social networks in December 2009. Third, Facebook explained the policy change to each user at the next login and subsequently asked users to go over their privacy selections to review and update them, eliminating the concern that some users were not aware of the change. Fourth, the privacy policy changes in 2005, 2006, and 2007 did not bring new privacy tools to allow users selective control over content they put on the site. They were purely intended to loosen default access settings to directly achieve openness in sharing. Finally, the prior changes are outside the time frame of our data set and therefore do not overlap with our study period.[4]

Using a unique panel data set obtained from Facebook (Phan and Airoldi 2015), we first conduct regression discontinuity analyses to verify a discontinuous jump in context generation activities and disclosure patterns of Facebook users around the time of the policy change. We then estimate unobserved effects models to assess the immediate (instantaneous) and permanent (continuous) effects of the policy change. Our findings suggest that the introduction of granular privacy controls remarkably influenced users' content-sharing practices on the social networking site. This effect is not only discernible in the short run but also present in the long run. Specifically, in response to the change, the average user *increased* the use of wall posts and *decreased* the use of private messages. Furthermore, users' content-sharing activities resulted in *greater openness* or *decreased secrecy* in disclosures on the platform. However, we show that user-specific factors (i.e., network size, gender information, and prior disclosure patterns) shaped users' varying behavioral reactions to the policy change. Although users' behavior generally became more closed in terms of disclosure patterns as their friendship network grew, this trend was reversed after the change. Hence, the policy change was instrumental in alleviating the negative influence of network size on open disclosures, thereby fostering greater public exchange of information among users. We also observe that users who reveal (do not reveal) their gender are more (less) active in terms of content sharing, and more (less) open in terms of disclosure patterns. However, users who specify their gender (do not specify their gender) reduce (increase) their openness and become more (less) private in their disclosures after the change. Finally, we show that, in reaction to the change, users with exclusive prior disclosure patterns increase the use of wall posts and decrease the use of private messages. By contrast, users with inclusive prior disclosure patterns decrease the use of wall posts and increase the use of private messages. Taken together, our results suggest

[4] Facebook simplified its privacy settings in May 2010 (FB News Room 2010). Since this event overlaps with our long-run analysis, we control for the impact of this event in Section 6.

that the variation among *more* privacy sensitive users (those who do not reveal their gender and/or those who have exclusive disclosure patterns ex ante) and *less* privacy sensitive users (those who reveal their gender and/or those who have inclusive disclosure patterns ex ante) diminishes after the change, giving rise to a more homogeneous user base in terms of content-generation activities and disclosure patterns.

Overall, our empirical results support the argument of privacy critics about greater openness in disclosures with the privacy change. Although Facebook users, on average, appear to share more content via wall posts and less content via private messages than before, we show that some users, especially those who were less sensitive to privacy prior to the change, start sharing less content via wall posts and more content via private messages after the change. Thus, characterizing the privacy change event as a way to foster openness uniformly across all categories of users does not correctly depict the true influence of the change. The policy change has uniquely different impacts on various groups of users based on their sensitivity to privacy prior to the change, and this impact is not necessarily in the direction of increased openness.

In addition to providing strong empirical findings, our study makes significant contributions to the literature. Instead of characterizing information disclosure behavior in relation to mostly "static" data in user profiles, as operationalized in prior studies, for the first time we measure and use two types of "dynamic" content-generation activities with different degrees of sharing implications. Specifically, we depict disclosures in terms of *whom* the intended audience of revealed information is (based on the type of content-sharing activity) rather than *what* information is revealed. Second, rather than relying on experimental or survey data to study the relationship between privacy controls and intention to disclose, we use actual disclosure behavior observed on a popular OSN platform. The distinction is important because the privacy paradox suggests that individuals actually disclose more than their reported intentions. Third, we introduce a simple but powerful metric (called the disclosure index) that quantifies the openness of disclosure patterns based on the relative levels of different content-sharing activities.

We proceed with the literature review in the next section, followed by the development of our theoretical framework. We describe our research design and data set in Section 4. We perform the empirical analyses and show the results in Section 5. Section 6 goes over our robustness and internal validity checks. We discuss the implication of our findings in Section 7. Finally, we conclude the paper with a summary of the results and the limitations of our study in Section 8.

2. Literature Review

Digitization of information about every facet of our lives through information technologies brings unprecedented challenges to individuals' privacy.[5] Information, which was once ephemeral, can now have persistent imprints in the digital world (Tufekci 2008). Although people have expressed great concern for their privacy regarding involuntary information gathering by governments and corporations through constant surveillance of people's lives and actions, they have extensively and voluntarily shared sensitive information with others on OSN sites. The question of why people deliberately expose themselves to privacy threats by revealing personal details has puzzled privacy researchers. Scholars from the information technology, sociology, and psychology domains have made inquiries to address this question and uncover the reasons behind the seemingly contradictory behavior. Several factors have been highlighted as possible reasons explaining why people voluntarily disclose sensitive information in social networks, including social capital, pressure from peers and herding behavior, incomplete information about the consequences of revelation, lack of concern for privacy, trust in the service provider and members, and lack of understanding and, therefore, use of privacy settings (Donath and boyd 2004, Gross and Acquisti 2005).

Although there are many OSNs with various features and tools, appealing to different crowds with unique interests, profile pages of their users are the common denominator among all sites. A profile is "a representation of their sel[ves] (and, often, of their own social networks)—to others to peruse, with the intention of contacting or being contacted by others" (Gross and Acquisti 2005, p. 71). After joining an OSN, a user is asked a set of questions that help describe the user. In addition to contact information, the elements of profile data range from relatively innocuous fields (such as favorite music or book) to potentially sensitive fields (such as sexual orientation or political affinity). Early studies of online social networks examined privacy and disclosure behavior in relation to profile visibility because information revelation patterns indirectly capture the privacy choices of social network users, as "the information provided, its potential recipients, and its possible uses" have implications for privacy (Gross and Acquisti 2005, p. 73). The level of visibility of various pieces of profile data, or of the overall profile, was seen as equivalent to the level of disclosure.

Given that Facebook and Myspace were the most prominent online social network sites, especially among college students, early privacy studies on OSNs almost exclusively focused on the users of these sites.

[5] Please refer to Bélanger and Crossler (2011) and Smith et al. (2011) for an extensive review of the literature on information privacy.

However, the sites had major differences in default visibility settings. Facebook was partitioned into "networks," each representing a specific college. The default setting was that only people in one's own college (network) could see a user's full profile (i.e., a profile was visible to "everyone" in the network), while all other users could see only the user's profile picture, name of the network, and name provided in the profile. Because of the demarcation of the site into networks, Facebook was often referred to as a "walled garden" (Tufekci 2008, p. 22). Myspace, on the other hand, was open to everyone by default and therefore regarded as less private. In addition, no networks or subgroups were available. However, both sites allowed their users to restrict default permissive privacy (visibility) settings to "friends only," meaning that only users designated as a "friend" could access one's profile. Since the default visibility was "everyone" in the case of Myspace and "everyone in the network" in the case of Facebook, researchers examined user profiles to understand whether disclosure behavior restricts the audience to "friends only" or users choose not to reveal, and thereby withhold, information in some fields on their profile. Apart from collecting observational data, researchers also surveyed users, mainly college students, to infer the amount of information revealed and the use of privacy settings and to compare stated privacy attitudes with actual disclosure behavior. These studies collectively documented empirical evidence of widespread disclosure practices in the early days. Jones and Soltren (2005) found that more than half of the students disclosed information about their favorite books, music, and interests, but much less disclosed their phone numbers. Stutzman (2006) concluded that students overwhelmingly disclosed their birthdays, relationship status, and political views, while disclosure of cell phone numbers was limited. In addition to confirming the findings in other studies regarding high levels of disclosure of personal information on user profiles, Gross and Acquisti (2005) found that only a small set of users adjusted the default (permissive) privacy settings to restrict the visibility of their profiles. Acquisti and Gross (2006) argued that stated privacy concerns have little influence on information disclosures: Highly concerned users also reveal extensive information on their profiles. Taken together, these findings point out the dichotomy between stated privacy concerns and actual information sharing behavior. Lampe et al. (2006) reported that only 19% of profiles are set as "friends only." A survey study by Tufekci (2008) revealed that Facebook and Myspace users do not set their profile visibility in relation to the level of their general privacy concern, but the fear of unwanted audiences has an impact on profile visibility settings. However, perceived future audiences (e.g., romantic partners, employers, the government) have no impact on the visibility of their profiles, suggesting that although users are better at managing "spatial" boundaries by restricting the visibility of their profiles to current audiences, they are less concerned about, or aware of, intrusions through "temporal" boundaries by future audiences. Similar disclosure practices were found among Myspace users as well (Caverlee and Webb 2008, Thelwall 2008). Different from the studies exclusively focusing on one's own profile attributes and selected privacy settings, Lewis et al. (2008) examined whether relational factors (e.g., friendship and roommate ties) contribute to a student's choice of having a private profile over a public one. They defined a profile as private if the student changed the default settings so that the profile was not fully accessible or searchable by nonfriends in the same network, indicating privacy-preserving behavior by limiting visibility. They found that a student is more likely to have a private profile if the student's friends, especially roommates, have private profiles or the student is active on Facebook. Stutzman and Duffield (2010) concluded that having a friends-only profile is more likely for users with a large friend network, implying a potential inflection point in the number of friends beyond which users transform their profiles from open to friends only. Prior research also identified gender and racial differences in disclosing or withholding profile information, though the results were not convergent (or consistent) across studies (Acquisti and Gross 2006, Lewis et al. 2008, Tufekci 2008).

With an increased awareness about privacy threats and extensive coverage of these issues in the popular press, OSN users started exhibiting more privacy-seeking behavior over time (boyd and Hargittai 2010). Dey et al. (2012) found that a large fraction of profile pages of New York City Facebook users became more private (i.e., disclosing less information) between March 2010 and June 2011. Stutzman et al. (2012) documented the evolution of privacy and disclosure behavior. Examining the profiles of early Facebook adopters in the Carnegie Mellon University network over years, they concluded that users reduced the amount of personal information on their profiles shared with other unconnected users in the same network between 2005 and 2009. They also showed a reversal in the privacy-seeking trend after 2009 as users resumed public sharing of various elements of their profile data. Similar to our study, Stutzman et al. (2012) took a longitudinal perspective. However, our study differs from theirs in several key aspects. First, they considered how disclosure of personal information on user profiles has changed since the early days. Therefore, they focused on *profile elements*, such as birth date, political affiliation, and home address, not on *content-generating user activities* like the wall posts and private messages that we study. We exclusively focus on content-generation

activities and analyze the changing disclosure patterns in response to a specific policy change. Second, their study was mostly descriptive and questioned whether public disclosure of personal profile information has been influenced by the changes in the default privacy settings of Facebook. On the other hand, we build econometric models to study the link between privacy controls enabled by the policy change and user-generated contents and their patterns. Third, while they considered whether users reveal or withhold information on their profiles based on observations at different points in time (specifically, in seven yearly snapshots), we use content-generation activities recorded weekly across 192 weeks.

Researchers have also examined the question of whether privacy controls have any impact on privacy concerns and resulting disclosure behavior. Studying the reaction of Facebook users to the introduction of the News Feed feature, Hoadley et al. (2010) showed that users expressed a higher concern for privacy because they perceived a loss of control over personal information due to easier information access. Xu (2007) showed that perceived controls mitigate privacy concerns in the context of location-based services. Using survey-based experiments, Brandimarte et al. (2013) studied the relationship between perceived control over the release of personal information and individuals' willingness to disclosure information. They showed that people indeed revealed more (less) when they had more (less) control over the information they released. Consistent with prior studies, we attribute extensive information disclosure behavior of Facebook users after the policy change to the sense of control hypothesis.[6] Increased control over information disclosed results in higher levels of open content sharing because users feel confident in managing the privacy risk associated with information disclosure to customized audiences. However, unlike prior studies, we use observational data to assess the impact of a real privacy change on dynamic content-sharing activities, instead of assessing the impact on (mostly) static profile data. In addition, we show the impact of increased control on disclosure using a panel data set rather than cross-sectional data collected through surveys or experiments. Furthermore, we capture the actual sharing patterns of different types of user-generated content instead of individuals' perceptions and intentions, which can be collected through surveys. Hence, we assess information disclosure, and therefore privacy concerns, in terms of the openness and secrecy of content sharing rather than the willingness to disclose information in certain profile fields.

Managing disclosures across multiple social contexts has been identified as the main challenge of privacy regulation in OSN platforms, known as "context collapse" (Marwick and boyd 2011, p. 122). Individuals rely on technical, behavioral, and mental strategies in managing their privacy on social networking sites with the copresence of multiple social groups (Lampinen et al. 2006, 2011; Stutzman et al. 2012). The use of privacy controls and settings, which limit disclosure to selected audiences, is a technical solution to privacy. OSN users also perform self-censorship, which refers to withholding some types of disclosure, or use distinct communication channels (e.g., private messages versus public wall posts) in different sites. These are some of the behavioral strategies for privacy management. Furthermore, OSN users take advantage of mental strategies, such as the creation of more inclusive in-group identities, the reciprocity of trusting other users, and being responsible in sharing information. Our research argues that a policy change enhancing the controls made available to Facebook users as a tool in their technical strategy eventually influences their behavioral strategies in terms of disclosure patterns of shared content.

Given the lack of causality arguments (e.g., see Airoldi and Rubin 2017) in prior research to predict different visibility levels of profiles, mainly because of the cross-sectional nature of the analyses, Lewis (2011) used a longitudinal data set to study the coevaluation of friendship network and privacy behavior on Facebook. He showed that privacy behavior (adopting a private profile open to friends only) has no impact on the evolution of one's friendship network. On the contrary, peers with whom a user associates and the user's network position influence the privacy behavior of the user, which itself varies across time and context. A similar result regarding the network effect of friends on privacy behavior was also identified by Dey et al. (2012), who concluded that a user's decision to change privacy settings is influenced by the decisions of their friends.

3. Theoretical Development

In this section, we develop theoretical arguments for our empirical analyses. We first present our theoretical

[6] The sense of control has been discussed in various other domains. Peltzman (1975) argued that individuals tend to react to a safety regulation by increasing other risky behaviors, offsetting some or all of the benefits of the regulation. People also tend to overestimate their ability to affect the outcome of events when they can exercise control (Thompson 1999). For instance, people generally feel more comfortable when they are in the driver's seat (i.e., high-control situation) than the passenger seat (i.e., low-control situation). This perception is more pronounced when people have choices in terms of controls (Langer 1975). One possible explanation for this phenomenon is that people want to avoid the negative consequences associated with having no control over outcomes. Fischhoff et al. (1978) showed that perceived level of control also influences the relationship between risk perception and risk acceptance: the lack of control results in judging risks as more severe, whereas having control leads to evaluating risks as less severe than they actually are.

foundation based on the extant literature on privacy-related decision making that emphasizes the importance of balancing the pros and cons of information disclosure. We next discuss the underlying mechanism governing information disclosure drawing on the communication privacy management (CPM) theory, which conceptualizes how people manage disclosures through boundary controls to maintain a proper balance between openness and secrecy. Then, building on these arguments, we develop an analytical model to characterize the disclosure behavior in terms of wall posting and private messaging to predict how privacy controls influence these information-sharing activities and the resulting disclosure patterns of online social networking users. Finally, we state our hypotheses to be tested subsequently.

3.1. Privacy Calculus

Advances in information technology have permeated all aspects of individuals' lives. The increasing economic value of personal information causes concern about privacy when individuals share information with others (Milberg et al. 1995, Smith et al. 1996, Culnan and Armstrong 1999). Information privacy concerns affect various privacy-relevant behaviors, such as releasing personal information to a marketer (Malhotra et al. 2004), agreeing to be profiled by online vendors (Awad and Krishnan 2006), and disclosing personal health information (Anderson and Agarwal 2011). In the extant literature, managing information privacy is generally viewed as a cognitive/mental computation called *privacy calculus*, which harmonizes the contrasting forces stemming from the value associated with the information sharing and the risks associated with not concealing the information (Klopfer and Rubenstein 1977, Laufer and Wolfe 1977, Posner 1981, Culnan and Armstrong 1999). Drawing on social exchange theory (Emerson 1976) and expectancy theory of motivation (Vroom 1964), these studies posit that prior to sharing personal information with others, an individual considers positive and negative consequences of such information disclosure. This cost–benefit trade-off influences the privacy-relevant behaviors of individuals in different contexts, including online personalization (Chellappa and Sin 2005), e-commerce transactions (Dinev et al. 2006, Dinev and Hart 2006), online financial portals (Hann et al. 2007), and location-based services (Xu et al. 2009). Krasnova et al. (2010) showed that an individual's disclosure decisions in online social networks are also subject to privacy calculus. While the benefits depend on the context in which information exchange takes place (e.g., monetary reward, time saving, future convenience, relevance and appropriateness of offers and contents, social benefits such as relationship building, self-representation, enjoyment), the extant literature agrees that the cost of the information exchange mainly involves privacy concerns or risks. In this research, drawing on the prior studies on privacy calculus, we anchor our research framework in the tension between granting access to personal information to obtain benefits associated with disclosure and the ability to keep information private and secret to limit or eliminate risks that stem from privacy threats. The issue of balancing disclosures with privacy threats is complex (Petronio 1999). We rely on the CPM theory (Petronio 2002) to explain the mechanism through which various forms of information disclosure are managed in the context of online social networks.

3.2. Communications Privacy Management

Privacy is often defined as "the selective control of access to the self" (Altman 1975, p. 114) in the literature. Control and ownership of private information are interrelated concepts and salient aspects of privacy management. Controls determine who has access to information that belongs to us, preventing unwanted exposure. CPM theory suggests that people conceal or reveal their private information by coordinating interpersonal boundaries (Petronio 2002). While thick boundaries maintain high levels of control to promote secrecy, thin boundaries deploy fewer controls to facilitate openness. If information is private, one has strong control over personal information and subsequently the boundary becomes very tight. One can choose to share private information with one or more people. Those who are privy to such information become a part of one's cognitive information space with a clearly defined boundary. When the boundary is lax (tight), more (fewer) people are within the information space. This requires individuals to perform a cognitive calculus to determine whether to reveal or conceal their information and to whom to reveal it (Laufer and Wolfe 1977). In doing so, they consider the benefits, such as social capital, and the costs, such as the risk of misuse of private information (Petronio 2002, Margulis 2003). CPM theory highlights the dialectical tensions between openness and secrecy. There is the need to be private through concealing and also the need to be public through revealing (Petronio 2002).

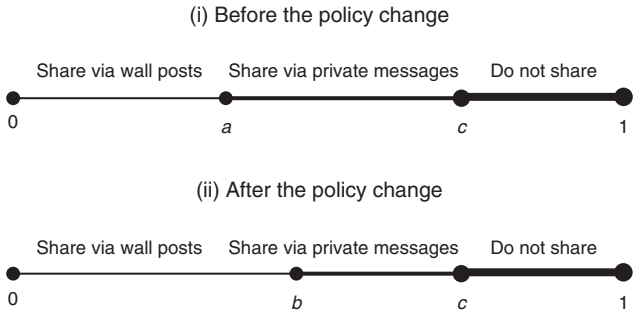
Once a person discloses private information, that person becomes a little bit less private/more public. Therefore, an action toward disclosing is also an action against privacy. On OSNs, people always reveal information. We cannot observe what information people conceal. However, while sharing information with others, people can choose with whom to share. People can tightly control their boundaries by sending private messages, which reflects *closedness* (*secrecy*) *in sharing*. Alternatively, people can loosely control their boundaries by making wall posts, which captures *openness in sharing*. Based on the behavioral responses of users

across the dichotomy between private messaging and wall posting, we define a metric to summarize the degree to which users disclose content: *disclosure index*, a proxy for the sharing pattern of a user in terms of content-generation activities with different intended audiences, defined as the ratio of the number of wall posts to the number of private messages. This ratio represents the tightness/looseness of the boundary around information that is shared with others. The higher (lower) the disclosure index, the more open (secret) the individual is in a given period in terms of content-sharing activities.[7]

We expound on our theoretical arguments in reference to our metrics as follows. Suppose that we represent the information set of a user with respect to information sensitivity as a normalized line, depicted in Figure 1, capturing the sensitivity of information along the x-axis. The thickness of the line around the information set represents the boundary controls deployed to protect the secrecy of information. The higher the sensitivity of information, the tighter the controls around the information and, therefore, the less likely that information is revealed to one or more users through the OSN platform. The user does not share some information that is highly sensitive (labeled "do not share") with anyone. This set might include pieces of information about sexual preferences, unhappy moments, financial details, or private family matters. On the other hand, the user has some information that is sensitive but can be shared with selected users (labeled "share via private messages"). For instance, the user can share personal health problems with close friends via private messages. Hence, the user relaxes the control over personal information to make exceptions. Furthermore, certain information can be considered less sensitive and therefore can be shared with many people through wall posts (labeled "share via wall posts"). As a result, the controls around the boundary of this less sensitive information are set loose.

After the Facebook change in their privacy policy and the provision of more granular controls, the user sees more control over sharing behavior because the user can effectively choose the audience for information revealed through each wall post. Because the user does not have to rely on the same setting for every wall post, the user can manage privacy risks more effectively and subsequently disclose a larger fraction of personal information via wall posts; that is, by using wall posts, the user shares a portion of the information that was previous shared using private messages

Figure 1 Information Sensitivity, Boundary Controls, and Disclosure Behavior



because of the lack of granular privacy controls. However, the inclusion of new privacy controls does not affect the information set that the user does not share with anyone as the new controls do not change the sensitivity of information per se. With the policy change, while the *closedness* (*secrecy*) *in sharing* decreases from $(c-a)$ to $(c-b)$, the *openness in sharing* increases from a to b. As a result, the *disclosure index*, which is the ratio of openness in sharing to closedness in sharing increases from $a/(c-a)$ to $b/(c-b)$. Hence, once an individual perceives that they are better equipped with controls to manage privacy, the user is likely to loosen the boundary surrounding private information. The privacy event opens up the boundary of information set previously as shared exclusively. Users share less information via private messages and more information via wall posts.

We argue that the late 2009 privacy policy change afforded users more granular controls over the sharing of their information and subsequently affected the users' ability to control the privacy of their information. Consistent with privacy calculus and CPM theory, we postulate that the policy change causes broader information exchange among Facebook users, in which individuals become less private and more public in their content-sharing activities and, therefore, use fewer private messages and more wall posts. As a result, disclosure patterns reflect greater openness in content sharing.

3.3. An Analytical Model

In this section, we build on our theoretical arguments to develop a stylized model to analyze the impact of the Facebook privacy change on the disclosure behavior of Facebook users. Our objective is to characterize social network users' information-sharing decisions within a simple utility framework to generate testable hypotheses for the empirical analysis that follows.[8]

[7] We believe the index can be extended to include other activities such as "tags" and "check-ins." However, for our research, we limit it to the two most popular content-generation activities, which are also the most mature and generalizable to other OSNs.

[8] Facebook users may also receive utility from information consumption (i.e., reading of information shared by others). However, we do not observe the consumption part. Fully characterizing

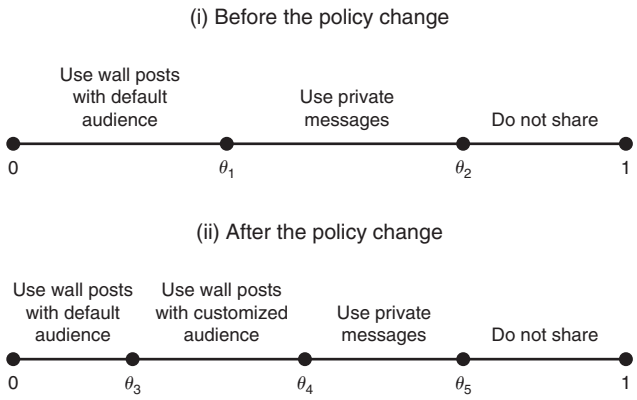
Our theoretical model is kept intentionally simple to capture the intuition of how Facebook's policy change and other factors influence different content-sharing activities of users. In our model, we assume that a Facebook user earns utility from sharing information via wall posts and private messages.[9] We represent the utility of a user derived from sharing information on Facebook with $u(\theta) = \alpha X - \beta X^2\theta$, where $\theta \sim U[0,1]$ captures the sensitivity of the shared information.[10] The utility function has two components: benefit and cost. The user gains a benefit from engaging in sharing activities in the social networking platform. The user also incurs a cost from disclosure because shared content can be misused, causing privacy-related losses. The benefit, captured by αX, depends on the marginal value of sharing information with others, α, and the audience (i.e., number of recipients) of shared information, X. Obviously, a wall post, reaches a larger audience than a message. The cost, denoted by $\beta X^2\theta$, depends on the privacy risk perception/sensitivity of the user, β. The cost element also includes the square of the audience, X^2, and the information sensitivity of shared content, θ. We take the square of the number of recipients because shared content can be misused not only by people who are the direct recipients but also by others with whom direct recipients can share the content. Hence, the quadratic term accounts for indirect losses.

Before the privacy policy change, when a user shares information using a wall post, we assume that it reaches $f(N)$ other users, where N is the number of Facebook friends of the user and $f(N) \geq N$, $f'(N) > 0$. The functional form, and therefore value, of f is determined by the visibility of wall posts set by the user in their profile, which can be "only friends" or "friends of friends." On the other hand, when the user shares information using a private message, we assume that it is directed at a specific user only.[11] Therefore, we can write utility expressions for each sharing activity as follows:

$$u(\theta; \textit{before} \mid \textit{wall post}) = \alpha f(N) - \beta f(N)^2\theta,$$
$$u(\theta; \textit{before} \mid \textit{message}) = \alpha - \beta\theta.$$

Comparing these expressions for each level of sensitivity to solve for the optimal sharing decisions, we can show that the user shares (i) content of *low* information sensitivity via wall posts (i.e., $\theta \leq \theta_1$), (ii) content of *medium* information sensitivity via private messages (i.e., $\theta_1 < \theta \leq \theta_2$), and (iii) no content with other users if information sensitivity is *high* (i.e., $\theta > \theta_2$). Figure 2(i) depicts these regions of sharing activities before the privacy change, where the cutoff values of information sensitivity are $\theta_1 = \alpha/(\beta[f(N)+1])$ and $\theta_2 = \alpha/\beta$.[12]

Figure 2 **Optimal Disclosure Behavior Based on Information Sensitivity**



After the policy change, the user does not have to go with the same audience for each wall post and has the option to customize the recipients of wall posts. For instance, the user can share a wall post with a subset of Facebook friends $g(N)$, such as buddies, work acquaintances, or family members, where $g(N) < N$ and $g'(N) > 0$. The user can also share wall posts with $f(N)$ users without customizing the audience. In addition, the user can share content using a message, as before. Hence, the utility expressions from various sharing activities are as follows:

$$u(\theta; \textit{after} \mid \textit{wall post}, \textit{default audience}) = \alpha f(N) - \beta f(N)^2\theta,$$
$$u(\theta; \textit{after} \mid \textit{wall post}, \textit{customized audience}) = \alpha g(N) - \beta g(N)^2\theta,$$
$$u(\theta; \textit{after} \mid \textit{message}) = \alpha - \beta\theta.$$

Again comparing the utility expressions above, we can show that, in the optimum, the user shares (i) content of *very low* information sensitivity via wall posts and does not customize the audience (i.e., $\theta \leq \theta_3$), (ii) content with *low* to *medium* sensitivity via wall posts and customizes the audience using privacy controls (i.e., $\theta_3 < \theta \leq \theta_4$), and (iii) content with *medium* to *high* sensitivity via private messages (i.e., $\theta_4 < \theta \leq \theta_5$). Finally, the user does not share content if its sensitivity is *very high* (i.e., $\theta > \theta_5$). Figure 2(ii) depicts these regions of sharing activities after the privacy change,

Facebook users' information-sharing and consumption decisions in a comprehensive model is beyond the scope of this paper.

[9] Shared information refers to any content that the user generates, such as comments, links, photos, and videos.

[10] The probability density function for the sensitivity of shared information can follow any distribution. We use the uniform distribution for tractability reasons.

[11] A private message can also be sent to multiple users. Capturing this possibility in the model complicates the model without changing the qualitative nature of predictions from the model.

[12] It is reasonable to assume that $\alpha < \beta$. Otherwise, the user reveals every piece of their private information.

where the cutoff values of information sensitivity are $\theta_3 = \alpha/(\beta[f(N)+g(N)])$, $\theta_4 = \alpha/(\beta[g(N)+1])$, and $\theta_5 = \alpha/\beta$.

We can make a number of observations based on the analytical results and develop testable hypotheses.

Wall Posts. We observe that users generate θ_1 wall posts before the change and θ_4 after the change. It is easy to show that $\theta_1 < \theta_4$. The introduction of granular privacy controls changes wall posts in two ways. First, some content (specifically, $\theta_1 < \theta < \theta_4$) that was previously shared using messages due to the lack of granular privacy controls is now shared using wall posts by choosing a customized audience. Second, users use fewer wall posts to share content with the same audience specified in their visibility settings; that is, they customize the audience for some wall posts that were previously shared with a larger (default) audience (specifically, $\theta_3 < \theta < \theta_1$). Overall, users start sharing a larger fraction of content using wall posts. Formally, we state the following.

Hypothesis 1 (H1). *The Facebook privacy policy change increases the use of wall posts*.

Private Messages. Although new privacy controls enable users to substitute some private messaging activities with customized wall posts, they do not cause users to share any new content that was deemed too sensitive before the change through private messages. Based on the results, users generate $\theta_2 - \theta_1$ messages before the policy change and $\theta_5 - \theta_4$ messages after the change. It is obvious that $\theta_5 - \theta_4 < \theta_2 - \theta_1$. Therefore, the Facebook policy change affects private messaging activity negatively. Thus, we hypothesize as follows.

Hypothesis 2 (H2). *The Facebook privacy policy change decreases the use of private messages*.

Disclosure Index. With the policy change, while *closedness* (*secrecy*) *in sharing* decreases from $\theta_2 - \theta_1$ to $\theta_5 - \theta_4$, *openness in sharing* increases from θ_1 to θ_4. As a result, the *disclosure index*, which is the ratio of openness in sharing to closedness in sharing, increases from $\theta_1/(\theta_2 - \theta_1)$ to $\theta_4/(\theta_5 - \theta_4)$. Hence, the privacy event opens up the boundary of the information set that was previously shared exclusively. Users share less information secretly and more information openly. Therefore, we formally state the following:

Hypothesis 3 (H3). *The Facebook privacy policy change increases the openness of disclosures*.

Friends on Sharing Activities and Disclosure Index. In addition to quantifying the impact of the policy change on wall posts, messages, and the disclosure index, we can also predict the effect of group size of Facebook friends on content-sharing activities and the resulting disclosure index. We observe from the model that users choose to share less content using wall posts as the friend network size increases (i.e., $\partial\theta_1/\partial N < 0$ and $\partial\theta_4/\partial N < 0$). By contrast, users prefer to share more content using messages as the friend network size increases (i.e., $\partial(\theta_2 - \theta_1)/\partial N > 0$ and $\partial(\theta_5 - \theta_4)/\partial N > 0$). Furthermore, the disclosure index decreases as the size of the friends network expands (i.e., $\partial(\theta_1/(\theta_2 - \theta_1))/\partial N < 0$ and $(\theta_4/(\theta_5 - \theta_4))/\partial N < 0$). These predictions hold in the period before the policy change as well as in the period after the policy change. Hence, as the network of Facebook friends grows, we conclude that users share less content via wall posts and more content via private messages and the openness of their disclosures drops. Therefore, we formally state the following:

Hypothesis 4A (H4A). *Growth in the Facebook friendship network decreases the use of wall posts*.

Hypothesis 4B (H4B). *Growth in the Facebook friendship network increases the use of private messages*.

Hypothesis 4C (H4C). *Growth in the Facebook friendship network decreases the openness of disclosures*.

4. Data and Experiment

4.1. Experimental Research Design

We use a quasi-experimental design in which disclosure-related outcomes (i.e., dependent variables) are measured over time for Facebook users. We collect data on different types of disclosures at multiple consecutive points before and after the introduction of the new privacy policy (i.e., treatment or intervention). Specifically, we use a *single-group interrupted time-series* experimental design (Cook and Campbell 1979) to compare the patterns of disclosure behaviors of Facebook users. In this design, disclosure-related outcomes before the treatment (i.e., pretreatment observations) are used as a baseline to assess the impact on the same outcomes after the treatment (i.e., posttreatment observations). The intervention, or treatment, effect is demonstrated if the pattern of posttreatment outcomes differs from the pattern of pretreatment outcomes. This design is particularly effective in identifying the type of impact (*instantaneous* or *delayed*), if any, as well as the permanence of the impact (*continuous* or *discontinuous*) when a large number of observations for the outcomes of interest are available (Cook and Campbell 1979, Gillings et al. 1981). This enables evaluation of the effects of policy interventions in circumstances in which randomized experiments are simply impractical and/or interventions are natural (like ours), dictating that all users of the study population be exposed to the intervention at once, thereby eliminating the possibility of having a separate control group (Michielutte et al. 2000). Under these circumstances, an interrupted time-series design is a viable alternative to true experiments because it has many pre- and postintervention observations, and this permits it to distinguish a true intervention effect

from a time trend or seasonality (Cook and Campbell 1979, Glass 1997). This design has become the standard method of causal analysis in applied behavioral research (Glass 1997). Prior studies involving public policy interventions have successfully used this design to evaluate the effectiveness of alcohol treatment programs (Berman et al. 1984), healthy diet programs (Coates et al. 1981), Medicaid reimbursement procedures on nursing home costs (Coburn et al. 1993), and traffic measures on fatality rates (Ross et al. 1970).

4.2. Data Description

Through collaboration with Facebook, we first identified Facebook users who attended college anytime during the 2007–2011 academic years and signed up on Facebook before the privacy change event. This search resulted in more than 1.3 million active users. Because of the sheer volume, we confined our further data collection to college users who indicated college X, which is a medium-sized private research institution in the Northeast, as their network. The resulting user set consisted of 13,145 active users. Then we gathered profile information such as gender and the date of registration for each user in the user set. All user-identifiable information was anonymized. After that, we queried the friendship database to establish a dynamic network of number of friends in each week for each user. This was done based on the time stamp indicating when each relationship was confirmed. Finally, we queried the content database to quantify the level of private messaging and wall posting activity by each user. The number of messages and posts produced by each user was aggregated at a weekly level from September 3, 2007 (week 1), through May 23, 2011 (week 192). At the end, we obtained an unbalanced panel of 2,428,885 observations (user-week pairs) from 13,145 active users. The policy change on December 9, 2009, falls in week 119.

We use two different time frames to characterize the impact of the policy change on disclosure behaviors of Facebook users: *short run* and *long run*. Our short-run analysis investigates the immediate (instantaneous) impact of the policy change, while our long-run analysis assesses the continuous (permanent) impact of the change. Our objective is to understand whether the policy change has an impact that is (i) immediate and continuous (i.e., treatment effect in both short-run and long-run analyses), (ii) immediate and discontinuous (i.e., treatment effect in short-run analysis only), (iii) delayed (i.e., treatment effect in long-run analysis only), or (iv) none (i.e., no treatment effect in either analysis). Since controlling for time/cyclical and maturation trends requires a long baseline to establish these patterns (Cook and Campbell 1979, Glass 1997), we utilize all pretreatment observations in our analyses. For the short-run analysis, we use a window of six weeks after the policy change. On the other hand, we use all observations after the policy change for the long-run analysis.[13]

Table 1 Descriptive Statistics

Variable	Time period	Average	Std. dev.	Minimum	Maximum
Post	Before	1.820	5.594	0	273
	After (Short)	1.030	3.523	0	209
	After (Long)	0.806	2.856	0	248
Message	Before	1.890	9.260	0	496
	After (Short)	1.223	6.403	0	379
	After (Long)	1.029	6.000	0	471
OSNAge	Before	98.450	64.218	0	303
	After (Short)	154.267	59.315	50	310
	After (Long)	188.429	63.313	50	379
Friend	Before	100.477	154.802	0	1,453
	After (Short)	134.122	199.742	0	1,453
	After (Long)	149.993	222.400	0	1,582

We consider the two most popular content-generation activities with opposite sharing implications in terms of intended audience:[14] (i) wall posts and (ii) private messages. Wall posts, including status updates, pictures, and videos, by their nature have an intended audience of more than one user (facilitating *openness* in sharing), whereas private messages are typically directed at a particular user (facilitating *closedness* (*secrecy*) in sharing). In addition, other covariates may affect the content generation and disclosure patterns of users. These variables are *OSNAge* (number of weeks since a user joined Facebook), *gender* (not specified, female, male), and *friend* (number of friends of a user). Table 1 reports the descriptive statistics of our variables in different time periods.[15] Tables S1 and S2 in the online appendix (available as supplemental material at https://doi.org/10.1287/isre.2016.0672) present the correlation matrices.

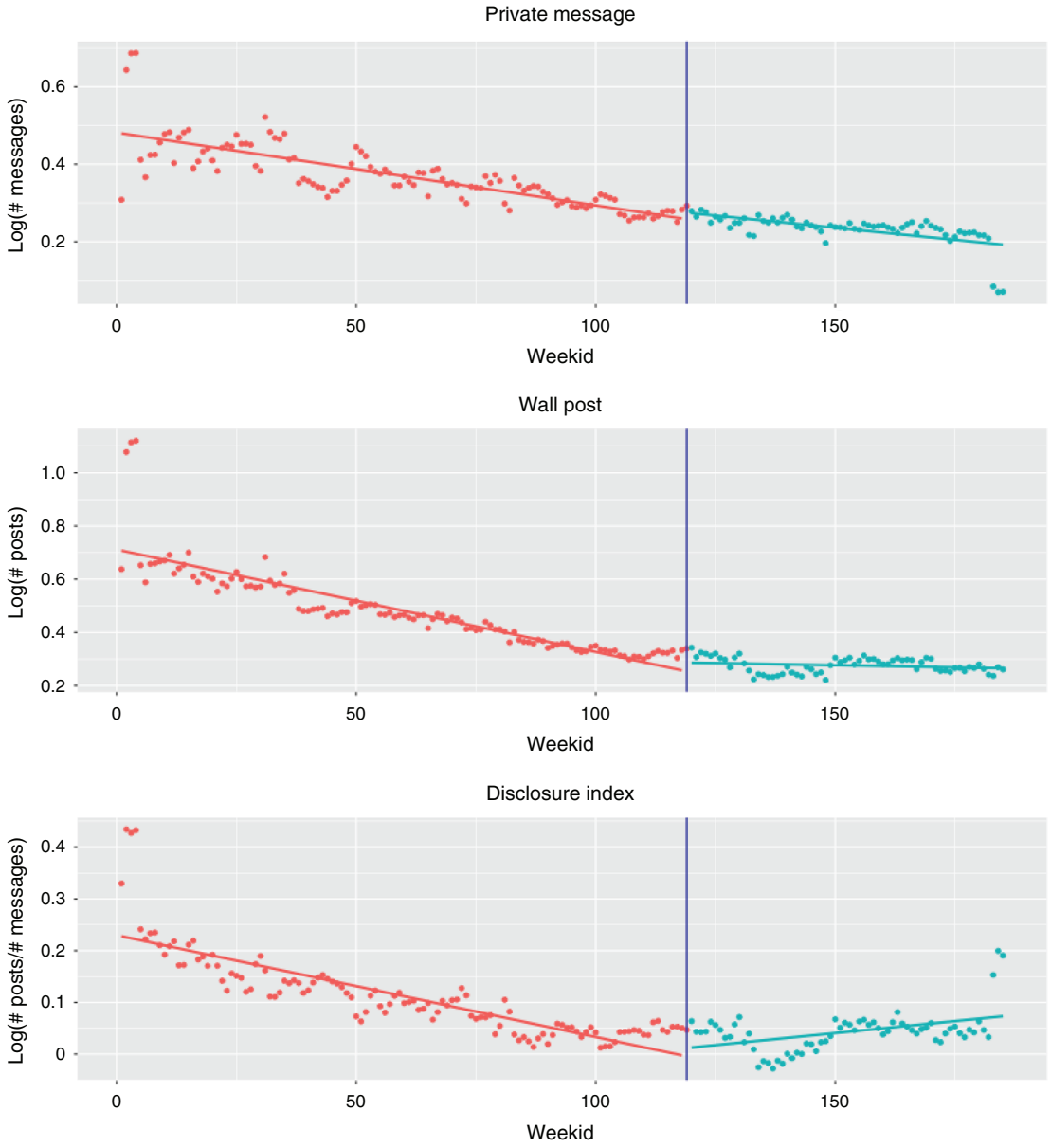
Since the periods before and after the change can have unique time trends, we cannot directly compare the frequencies of activities in these periods. However, we can observe that the average number of posts and the average number of messages decreased over time. In addition, we observe that deviation across observations within each content-generation activity dropped significantly with time. As for the friendship network, we see that users, on average, had more friends over time.

[13] We consider alternative posttreatment windows for the robustness check in Section 6.

[14] Based on our conversion with Facebook executives, "wall posts" and "private messages" are by far the most common activities generating user content on the OSN platform.

[15] Since *gender* is time invariant, we do not report it in Table 1. While 28.6% of users are female, 26.4% of users are male. The rest of the users do not disclose their gender.

Figure 3 (Color online) Average Disclosure Behavior Surrounding the December 9, 2009, Policy Change



Before we estimate various econometric models to test our hypotheses, we first plot the average number of messages, posts, and disclosure indices across weeks in Figure 3 to see the trends and fluctuations in disclosure behavior over time. These plots also give us a means to visually examine the impact of the policy change. The vertical blue lines in the figure indicate the week of the policy change. We also fitted linear trends to the data before and after the change. We can clearly observe that the trends and the intercepts for both the activity levels and the disclosure index are changing. Specifically, the policy change appears to lessen the downward trend in the number of posts and the disclosure index; that is, the coefficient of the trend line is significantly larger after the policy change for the posting activity and the disclosure index. Furthermore, there is a positive jump of the intercept around the week of the policy change for these two variables. Although there are also changes in the trend and the intercept for the messaging activity, these changes are not so obvious from the figure. All of these observations are consistent with our projections and thus give us initial evidence of the structural change resulting from the policy effect. However, visual observations cannot be sufficient for testing our hypotheses. In Section 5, we run various econometric models, first to verify the causality and then to estimate the influence of the policy change to formally test our hypotheses.

5. Analyses and Results

We analyze the potential impact of the policy change on three dependent variables: (i) *wall posts*, (ii) *private messages*, and (iii) *disclosure index*. We label the total number of private messages that user i sends in week t, $Message_{it}$. Similarly, we label the total number of wall posts that user i sends in week t, $Post_{it}$. Using these two values, we define the ratio of $Post_{it}$ to $Message_{it}$ as the disclosure index, $Disclosure\ Index_{it}$, of a user in a given week. Although this relative index is simple, it captures valuable information about the sharing patterns of users in terms of different content-generation activities with varying scopes of reach. More specifically, the disclosure index provides the frequency of content shared via wall posts with respect to the content shared via private messages. Therefore, the higher the value of the index, the greater the openness of disclosure.

5.1. Regression Discontinuity Analyses

Regression discontinuity design (RDD) estimates a treatment effect where the treatment is determined by whether an observed "assignment" variable exceeds a known cutoff point (Lee and Lemieux 2010). The basic idea behind this research design is that individuals with the assignment variable just below the cutoff (i.e., those who did not receive the treatment) are good comparisons to, and therefore serve as a valid counterfactual for, those just above the cutoff (i.e., those who did receive the treatment). This simple reasoning suggests attributing the discontinuous jump in a dependent variable at the cutoff to the causal effect of the treatment. In our context, the assignment variable is a deterministic function of time, and every Facebook user is treated sharply at the time of the policy change. Following the idea of RDD, we compare users' sharing behavior around the policy change to see if the policy change has any causal effect.

Basically, we aim to quantify the difference between how Facebook users would have behaved had there been no policy change and how they actually behaved. The best answer to this question lies in the sharing behavior of users within a short window around the policy change. To that end, we only use observations six weeks before the change and six weeks after the change to conduct our RDD analyses.[16] We first adjust the dependent variable to take out individual heterogeneity.[17] Specifically, we subtract each individual's mean level of the dependent variable over the six weeks prior to the policy change from the dependent variable. Then we analyze those differences using RDD. Similar to Gottlieb et al. (2016), we estimate the standard parametric RDD equations of the form

$$y^*_{it} = \alpha + \beta\, AfterPolicy_t + \sum_{k=1}^{3} \gamma_k Week_t^k + \sum_{k=1}^{3} \delta_k Week_t^k \times AfterPolicy_t + \varepsilon_{it}, \quad (1)$$

where $y^*_{it} = y_{it} - \bar{y}_i$ is the adjusted outcome variable for user i in week t. We use the natural logarithms of our dependent variables, $y_{it} \in \{Message_{it}, Post_{it}, Disclosure\ Index_{it}\}$, as these variables are highly skewed.[18] We code $Week_t$ as the week of observation relative to the policy change week, and $AfterPolicy_t$ is an indicator variable equal to one if the observation is after the policy change. We fit a separate third-degree polynomial trend on each side of the discontinuity. Our primary interest is the coefficient on the postpolicy indicator. This coefficient reflects the size of the discontinuity in the outcome variable at the cutoff week. If the privacy policy change impacts the sharing behavior of Facebook users, we would expect it to be negative for *messages* and positive for *posts* and *disclosure index*. We estimate the model in Equation (1) for each of our dependent variables with pooled regression.

The results from the regression discontinuity analyses are reported in Table 2. Across all three dependent

Table 2 Regression Discontinuity Analyses on Content Generation and Disclosure

Dep. variable	Message (1)	Post (2)	Disclosure index (3)
AfterPolicy	−0.0709***	0.0186**	0.0895***
	(0.0222)	(0.0092)	(0.0268)
Time	0.0775***	0.0428***	−0.0347
	(0.0179)	(0.0145)	(0.0216)
$Time^2$	0.0261***	0.0128***	−0.0133*
	(0.0057)	(0.0046)	(0.0069)
$Time^3$	0.0025***	0.0011**	−0.0014**
	(0.0005)	(0.0004)	(0.0007)
Time × *AfterPolicy*	−0.0594**	−0.0953***	−0.0359
	(0.0253)	(0.0205)	(0.0305)
$Time^2$ × *AfterPolicy*	−0.0325***	0.0008	0.0333***
	(0.0081)	(0.0066)	(0.0098)
$Time^3$ × *AfterPolicy*	−0.0020**	−0.0022***	−0.0002
	(0.0008)	(0.0006)	(0.0009)
Constant	0.0607***	0.0362***	−0.0246
	(0.0157)	(0.0127)	(0.0189)
R-squared	0.0002	0.0003	0.0002

Notes. The sample includes 157,740 observations from 13,145 users. Robust standard errors are in parentheses.
*$p \le 0.1$; **$p \le 0.05$; ***$p \le 0.01$.

[16] The policy change occurs in the middle of week 119. Therefore, we exclude the observations from week 119.

[17] We thank Joshua D. Gottlieb for suggesting this approach.

[18] We add one to the numbers of weekly messages and posts before taking the logarithms as some numbers can be zero.

variables, we observe that the coefficient on *AfterPolicy* is statistically significant. Specifically, there is a discontinuous *negative* jump in the number of messages, and a discontinuous *positive* jump in the number of posts and the disclosure index. These results are consistent with our theoretical predictions that providing users with granular privacy controls spurs openness of their disclosure. Hence, RDD analyses present strong evidence of the causal effect of the privacy policy change on Facebook users' content generation and disclosure patterns.

After showing the structural change in sharing behavior in an RDD framework, we next assess the influence of the privacy policy change on Facebook users in a panel setting while controlling for relevant factors that might affect their behavior.

5.2. Short-Run Panel Analyses

In this section, we seek answers to the following questions: Does the policy change have an immediate effect on user content-generation activities and disclosure patterns? If so, what kind of influence does the privacy policy change facilitate? To assess the impact of the Facebook policy change, we build the unobserved effects panel model given in Equation (2)

$$y_{it} = \alpha_i + \beta_1 AfterPolicy_t + \beta_2 OSNAge_{it} + \sum_{k=1}^{11} \beta_{k+2} Monthk_t + \varepsilon_{it}, \quad (2)$$

where α_i captures the activity-specific unobserved heterogeneity of user i and $AfterPolicy_t$ is our privacy change indicator, as before. We include $OSNAge_{it}$ and $Monthk_t$ as control variables.[19] Finally, ε_{it} represents idiosyncratic errors with standard assumptions. We estimate the models with the fixed-effects (FE) specification using the least squares dummy variable estimator.

Table 3 reports the results regarding the immediate effect of the privacy policy change. Regardless of the specification, it is clear that the privacy change reduces the number of messages significantly (i.e., the coefficient of *AfterPolicy* in column (1) is negative and significant). On the other hand, the number of wall posts and the disclosure index increase with the policy change, and these effects are highly significant (i.e., the coefficient of *AfterPolicy* in columns (2) and (3) is positive and significant). Furthermore, as age on the platform increases, we see that both types of content-generation activities drop. However, the reduction is more pronounced in wall posts, and therefore the disclosure index decreases with tenure in the platform. Overall, our results are consistent with our model predictions. The policy change has a substantial structural impact on the information disclosure patterns as well as the amount of content-generation activities. Facebook users share more content using wall posts and less content using private messages after implementation of the privacy change. In addition, openness of users' disclosure increases following the policy change. Hence, the privacy change manifests itself in disclosure-related outcomes instantaneously.

[19] Taking January as the baseline month, we use a time dummy for each calendar month from February to December.

Table 3 Panel-Level Analyses on Content Generation and Disclosure in the Short Run

Dep. variable	Message (1)	Post (2)	Disclosure index (3)
AfterPolicy	−0.0115***	0.0297***	0.0412***
	(0.0027)	(0.0024)	(0.0032)
OSNAge	−0.0011***	−0.0027***	−0.0016***
	(0.0000)	(0.0000)	(0.0000)
Month effects	Included	Included	Included
Constant	0.4610***	0.7340***	0.2720***
	(0.0022)	(0.0019)	(0.0026)
R^2	0.452	0.620	0.224

Notes. The sample includes 1,535,025 observations from 13,145 users. Robust standard errors are in parentheses.
***$p < 0.01$.

5.3. Long-Run Panel Analyses

Although our results in Section 5.2 provide strong evidence of change in user disclosures, it is not clear if this influence on sharing behavior fades over time, and therefore is short lived or long lasting. Therefore, in this section, we assess the effect of the privacy policy change on content generation and disclosure behavior in the long run. The questions we ask are the following: Does the policy change have a continuous effect on user disclosure patterns? If so, what kind of influence does the policy change facilitate in terms of content generation and openness of content sharing? The results pertaining to the long-run analyses are presented in Table 4.

Table 4 Panel-Level Analyses on Content Generation and Disclosure in the Long Run

Dep. variable	Message (1)	Post (2)	Disclosure index (3)
AfterPolicy	−0.0134***	0.0419***	0.0553***
	(0.0015)	(0.0013)	(0.0017)
OSNAge	−0.0011***	−0.0023***	−0.0012***
	(0.0000)	(0.0000)	(0.0000)
Month effects	Included	Included	Included
Constant	0.4570***	0.6830***	0.2260***
	(0.0018)	(0.0015)	(0.0020)
R^2	0.394	0.575	0.193

Notes. The sample includes 2,428,885 observations from 13,145 users. Robust standard errors are in parentheses.
***$p < 0.01$.

We can observe from Table 4 a clear pattern in the results. The negative and significant coefficient of *AfterPolicy* in column (1) indicates that users generate fewer messages after the privacy change. The positive and significant coefficient of *AfterPolicy* in column (2) implies that users generate more wall posts after the privacy change. In addition, Facebook users become more open in terms of disclosure of shared content (i.e., coefficient of *AfterPolicy* in column (3) is positive and significant). As for the influence of users' tenure on the platform, we find that users share fewer wall posts and fewer private messages and the openness of their disclosures decreases over time as they gain experience. All of these results are in line with our expectations and also consistent with the results in the short run. Our findings provide strong evidence that the policy change has a lasting influence on content-generation activities and the resulting disclosure patterns of Facebook users, as predicted by our theoretical model; that is, users reduce the number of messages and increase the number of posts, which in turn results in an increase in the openness of disclosures. Overall, we conclude that the Facebook privacy policy change that brought granular privacy controls was instrumental in changing users' sharing activities and openness of disclosures in the short run as well as the long run. Hence, the effect of the policy change is characterized as both instantaneous and continuous. Our empirical findings overwhelmingly support our H1–H3.

5.4. Impact of Friendship Network on Content-Sharing and Disclosure Behavior

Users with different network sizes might have distinctive behavioral responses to the privacy change because network size has implications for the reach of users' wall posts. In general, users with more friends have a larger audience for their wall posts. Prior research has shown that network size, which varies over time, can drive the disclosure behavior of users in Facebook, while disclosure behavior does not affect the size of the friendship network (Lewis 2011). Therefore, we examine the impact of network size on content-sharing activities and disclosure behavior. We operationalize the network size with the number of friends of a user i in week t, $Friend_{it}$. In addition, we control for gender using gender dummies, $Male_i$ and $Female_i$.[20] Prior research has revealed that females differ from males in their taste for privacy (Acquisti and Gross 2006, Lewis et al. 2008) and therefore can have dissimilar information disclosure patterns. Specifically, we extend our baseline panel model and estimate the extended model in Equation (3) for each of our dependent variables

$$\begin{aligned} y_{it} = {} & \alpha_i + \beta_1 AfterPolicy_t + \beta_2 OSNAge_{it} + \beta_3 Friend_{it-1} \\ & + \beta_4 Friend_{it-1} \times AfterPolicy_t \\ & + \beta_5 Male_i \times AfterPolicy_t \\ & + \beta_6 Female_i \times AfterPolicy_t \\ & + \sum_{k=1}^{11} \beta_{k+6} Monthk_t + \varepsilon_{it}. \end{aligned} \tag{3}$$

Table 5 presents our estimation results. The negative coefficients of *Friend* and (*Friend* + *Friend* × *AfterPolicy*) in column (2) provide support for the claim that Facebook users generate fewer wall posts as their friendship network grows in both periods (i.e., before the change and after the change). Therefore, our H4A is fully supported. We observe that the coefficient of *Friend* in column (1) is positive, implying that Facebook users generate more private messages as their friendship network grows before the policy change. However, the total coefficient of (*Friend* + *Friend* × *AfterPolicy*) is negative, implying that Facebook users generate fewer private messages as their friendship network grows after the policy change. Hence, our H4B is only partially supported. As for the disclosure index, we note that the coefficients of *Friend* and (*Friend* + *Friend* × *AfterPolicy*) in column (3) are negative. Hence, the openness of disclosures decreases as the friendship network grows in both periods. Thus, our H4C is fully supported.

Although users with a large friendship network are more closed in terms of disclosure patterns (i.e., the disclosure index decreases with network size), the positive coefficient of the interaction term in column (3) suggests that highly connected users become less conservative and more open in their disclosures after the change. Although Facebook enables users to connect easily and increase their network size, it seems that this comes at the cost of decreased openness over time. A decrease in the disclosure index over network size implies that Facebook failed to motivate its users to engage more openly with others in the platform as their network size grew before the change. However, the policy change was instrumental in reducing the growth of closedness in disclosures and facilitated openness instead. Consistent with the findings in Sections 5.2 and 5.3, users generate less content and the openness of their disclosures decreases as they gain experience. As for the influence of gender, we observe that the policy change affects females and males differently in terms of the use of messages and similarly in terms of the use of wall posts, relative to the levels of these activities prior to the change. However, both genders reduce their openness and become a bit more private compared to prior disclosure patterns.

[20] Unlike today, specifying a gender to sign up for Facebook was not required in the past. Therefore, we have some users who do not have gender information. We used them as the baseline.

Table 5 The Impact of Friendship Network on Content Generation and Disclosure

Dep. variable	Message (1)	Post (2)	Disclosure index (3)
AfterPolicy	0.0707***	0.1420***	0.0716***
	(0.0018)	(0.0015)	(0.0021)
OSNAge	−0.0008***	−0.0016***	−0.0008***
	(0.0000)	(0.0000)	(0.0000)
Friend	0.0002***	−0.0008***	−0.0006***
	(0.0000)	(0.0000)	(0.0000)
Friend × *AfterPolicy*	−0.0007***	−0.0004***	0.0003***
	(0.0000)	(0.0000)	(0.0000)
Male × *AfterPolicy*	0.0454***	−0.0986***	−0.1440***
	(0.0021)	(0.0018)	(0.0025)
Female × *AfterPolicy*	−0.0360***	−0.1140***	−0.0783***
	(0.0021)	(0.0018)	(0.0025)
Month effects	Included	Included	Included
Constant	0.4490***	0.6930***	0.2440***
	(0.0018)	(0.0015)	(0.0021)
R^2	0.406	0.591	0.195

Notes. The sample includes 2,428,885 observations from 13,145 users. Robust standard errors are in parentheses.
***$p < 0.01$.

5.5. Subgroup Panel Analyses: Users with Different Prior Disclosure Patterns

Although the analyses in previous sections reveal that Facebook users, on average, react to the policy change by opening up their boundaries to be less private and more public in content sharing, it is possible that the level of reaction might be different for various groups of users based on ex ante privacy sensitivity, which is reflected in prior disclosure patterns. Specifically, a user with a history of open disclosure patterns may respond to the change differently than a user with a history of closed disclosure patterns. Therefore, the reaction induced by the policy change may differ depending on the category of user in terms of prior disclosure patterns. One can argue that users who perceive more benefit from the change are affected more by the policy change. Specifically, those who were more private and less public in content sharing (i.e., those with a lower disclosure index) before the change might loosen their privacy boundaries to a larger extent. The argument is simple: Users who are more closed in their disclosures before are more likely to feel empowered by privacy controls to manage their privacy and/or use the granular controls brought by the privacy policy change to properly choose the audience for their posts. Hence, the policy change is expected to induce more wall posts and less private messages from these users relative to the users who are more open in their disclosures. To examine this issue, we estimate panel models with threegroups of users based on prior disclosure patterns: (i) those who are highly inclusive, (ii) those who are highly exclusive, and (iii) those who are in between prior to the policy change. We first calculate the average disclosure index, which is a reverse proxy for privacy sensitivity in terms of content-sharing behavior, for each user using disclosure patterns data before the policy change. Then we rank and identify 10% of users with the lowest (highest) average disclosure index and call this group the high (low) privacy sensitive group.[21] We call the rest the baseline group. We use the binary variables *Bottom*10 and *Top*10 for the low and high privacy sensitive groups, respectively, and subsequently estimate the following panel model in Equation (4) for each dependent variable:

$$\begin{aligned} y_{it} = {} & \alpha_i + \beta_1 AfterPolicy_t + \beta_2 OSNAge_{it} + \beta_3 Friend_{it-1} \\ & + \beta_4 Friend_{it-1} \times AfterPolicy_t \\ & + \beta_5 Male_i \times AfterPolicy_t \\ & + \beta_6 Female_i \times AfterPolicy_t \\ & + \beta_7 Top10_i \times AfterPolicy_t \\ & + \beta_8 Bottom10_i \times AfterPolicy_t \\ & + \sum_{k=1}^{11} \beta_{k+8} Monthk_t + \varepsilon_{it}. \end{aligned} \tag{4}$$

We can characterize the influence of the policy change on different subgroups of users by examining the interaction terms in Table 6. We see that, in response to the change, the high privacy sensitive group reduces the number of private messages and increases the number of wall posts (i.e., the interaction term *Top*10 × *AfterPolicy* is negative and significant in column (1) and is positive and significant in column (2)). By contrast, the low privacy sensitive group increases the number of private messages and reduces the number of wall posts (i.e., the interaction term *Bottom*10 × *AfterPolicy* is positive and significant in column (1) and is negative and significant in column (2)). Consistent with the results regarding the impacts of privacy sensitivity on content-generation activities, the disclosure index drops for the low privacy sensitive group and increases for the high privacy sensitive group after the change (i.e., *Top*10 × *AfterPolicy* is positive and significant and *Bottom*10 × *AfterPolicy* is negative and significant in column (3)). Thus, we can conclude that the level of reaction to the privacy change does indeed differ for users with different prior privacy sensitivity. The high privacy sensitive group responds to the change by sharing more content using wall posts and less content using private messages. Also, the low privacy sensitive group responds to the change by sharing more content using private messages and less

[21] We conducted robustness checks in Section 6 using different percentages. We obtained qualitatively similar results.

Table 6 The Impact of the Privacy Change on Users with Different Levels of Privacy Sensitivity

Dep. variable	Message (1)	Post (2)	Disclosure index (3)
AfterPolicy	0.0718***	0.1450***	0.0729***
	(0.00018)	(0.0015)	(0.0021)
OSNAge	−0.0008***	−0.0016***	−0.0008***
	(0.0000)	(0.0000)	(0.0000)
*Top*10 × *AfterPolicy*	−0.2570***	0.0158***	0.2730***
	(0.0028)	(0.0023)	(0.0032)
*Bottom*10 × *AfterPolicy*	0.0686***	−0.2530***	−0.3220***
	(0.0029)	(0.0024)	(0.0033)
Friend	−0.0002***	−0.0008***	−0.0005***
	(0.0000)	(0.0000)	(0.0000)
Friend × *AfterPolicy*	−0.0007***	−0.0003***	0.0004***
	(0.0000)	(0.0000)	(0.0000)
Male × *AfterPolicy*	0.0862***	−0.0954***	−0.1820***
	(0.0022)	(0.0019)	(0.0026)
Female × *AfterPolicy*	−0.0171***	−0.0943***	−0.0772***
	(0.0022)	(0.0018)	(0.0025)
Month effects	Included	Included	Included
Constant	0.4490***	0.6930***	0.2450***
	(0.0018)	(0.0015)	(0.0021)
R^2	0.409	0.593	0.203

Notes. The sample includes 2,428,885 observations from 13,145 users. Robust standard errors are in parentheses.

***$p < 0.01$.

content using wall posts. As a result, the variation among users in terms of disclosure patterns is reduced after the change, giving rise to a more homogeneous user base.

6. Robustness Checks

We performed a significant number of tests to confirm that our findings are due to the privacy policy change, thereby eliminating alternative explanations, and are robust to different specifications. We present the results for the dependent variables (i) *messages*, (ii) *posts*, and (iii) *disclosure index* in Tables A.1–A.3 in the appendix, respectively. Below we refer to the column number of each test in reference to these tables.

First, we use a FE specification to estimate our panel models to test our hypotheses in Section 5. We also estimate the base models with a random-effects (RE) specification using the feasible generalized least squares estimator. The results reported in columns (1) and (2) suggest that the qualitative nature of the results are the same regardless of the model specification. Second, our models in the analysis part captures the "average" effect of the policy change over the study period. We also estimate our models of the short-term analysis using weekly policy dummies (instead of a single policy dummy that captures the average effect) to see if the results hold for each week after the policy change. The estimations presented in column (3) imply that we get similar results with a weekly operationalization of the policy effect. Out of 18 weekly policy coefficients across 3 dependent variables, 16 coefficients are significant in the direction we expect. There is no coefficient that is both significant and inconsistent with our theoretical predictions. Hence, tracing out the impact of the policy change in a more granular manner does not change the results qualitatively. Third, we use robust standard errors in our estimations in Section 5. We also estimate our base models using standard errors clustered at individual levels. The results in columns (4) and (5) suggest that the clustered errors do not change the significance of the estimated coefficients. Fourth, our choice of time windows for the short-run and long-run analyses might be too specific and we may not obtain similar results if we choose different windows. Therefore, we repeat the analyses using alternative time windows. Specifically, we estimate the base models for the short-run analysis using windows of four and eight weeks (reported in columns (6) and (7)). We also estimate the base models for the long-run analysis using a window of 52 weeks (reported in column (8)). We obtain qualitatively similar results.

Fifth, our privacy dummy may be significant in our tested models because the induced reaction might have started even before the enactment of the change on December 9, 2009. If the observed reaction in content generation and disclosure were truly caused by our privacy event, we would expect no significant reaction to a "bogus" policy change. To that end, we perform a falsification test. We test our panel models assuming that a policy change occurred six months prior to the real event. As reported in column (9), we find that the bogus event had no significant effect on the number of messages, the number of wall posts, or the disclosure index. Sixth, although our disclosure index captures individual-level heterogeneity and the model specifications control for activity-specific unobserved heterogeneity of users, our results might still be driven by users who generate much more content than the average user(s) whose friend networks are much larger than the average. To eliminate the effect of potential outliers, we remove the observations where the average weekly number of messages or wall posts is more than four standard deviations above the mean before the policy change and repeat the analysis (reported in columns (10) and (11)). We also eliminate users whose average number of friends is more than four standard deviations above the mean before the policy change and redo the analysis (reported in columns (12) and (13)). The new analyses with reduced data sets indicate that our results do not change qualitatively.

Seventh, to be able to see the effect of time-invariant variables on content sharing and disclosure, we estimate the extended models and the models for the subgroup analysis using the feasible generalized least squares estimation. The results reported in column (14)

show that both males and females are more socially active in terms of content production, and are more open in terms of disclosure patterns, than users who do not specify their gender. This is intuitive given that users who choose not to reveal their gender may, in general, be more privacy conscious ex ante. However, users who reveal their gender reduce their openness and become a bit more private in their disclosures after the change. Hence, we can conclude that the policy change is also effective in reducing the ex ante difference in disclosure patterns between less privacy conscious users (i.e., those who reveal their gender) and more privacy conscious users (i.e., those who do not reveal their gender). Furthermore, the results in column (15) indicate that users who are more exclusive in content sharing generate more private messages and fewer wall posts than users who are more inclusive in content sharing. In addition, the openness of disclosure is greater for the low privacy sensitive group relative to the openness of disclosure for the high privacy sensitive group. These results are in line with our expectations. Ex ante privacy differences are reflected in content-sharing activities and the resulting disclosure patterns.

Eighth, in our subgroup analysis, we categorize users into high and low privacy sensitive groups by considering 10% of users from each end of the spectrum on average disclosure patterns before the policy change. To make sure that our results regarding the impact of privacy sensitivity are not driven by the selection of this cutoff, we estimate the models using alternative percentages. Specifically, we consider 5% and 20% of users instead of 10%. The results reported in columns (16) and (17) imply that we get qualitatively similar results, and hence our results are robust. Ninth, we control for time trend in activity levels using the age of Facebook users. However, this approach implicitly assumes that time trend is linear and monotonic.[22] To ensure that our linearity assumption in time trend does not bring any bias to our estimations, we added year dummies to our panel models to account for a possible nonmonotonic trend in time. We performed base, extended, and subgroup analyses again. The results given in columns (21)–(23) reveal that adding year dummies does not change the sign or significance of the estimated coefficients for hypothesized variables. Tenth, two of our dependent variables (i.e., *message* and *post*) are count variables. Since they take on a value from a large range, we use log transformation and linear models with FE and RE specifications. We also use linear models because our third variable, *disclosure index*, is not a count variable, and we seek consistency in interpreting the coefficients across the estimation models with different dependent variables. To ensure that our linear projection does not bring directional bias to estimations, we also estimate the models with count variables using Poisson regression. Our results reported in columns (24) and (25) indicate that the qualitative findings remain the same. Eleventh, one can argue that a fraction of Facebook users may not be worried about privacy at all and therefore are not affected by any privacy policy change. Hence, the impact of the change is less likely on these privacy insensitive users. In this case, our results regarding the effect of the policy change on content sharing and disclosure patterns should be considered downward biased; that is, the true effect on disclosure behavior is much stronger than what is found in this study.

[22] We thank an anonymous reviewer for bringing this point to our attention.

6.1. Internal Validity

Many confounding variables are ruled out as alternative explanations in the interrupted time-series design, as pre- and posttreatment outcomes do not differ on most confounding variables (Johnson and Christensen 2010). Hence, this design, based on comparison within the group, addresses the majority of internal validity threats (Community Tool Box 2014). However, some challenges to the internal validity exist (Forastiere et al. 2016). The potential threats to internal validity are *mortality* (i.e., did some subjects drop out after the intervention?), *maturation* (i.e., were changes in the dependent variables due to a normal development process of subjects?), *time trend/seasonal effect* (i.e., were changes in the dependent variables due to a time effect or seasonal trend?), *statistical regression* (i.e., did subjects come from low- or high-performing groups?), and *history* (i.e., did other current events affect the change in the dependent variables?) (Cook and Campbell 1979). We rule out these potential threats in a systematic manner to ascertain that the privacy event we study is the true cause of the change in content sharing and disclosure behavior.

First, mortality is not an issue for our study because we employ the same set of users before and after the policy change. Therefore, there is no attrition problem, eliminating the alternative interpretation that a different composition of the experiment group in the pretreatment and posttreatment periods caused the observed effect. Second, one can argue that Facebook users change their disclosure behavior as they gain experience or grow older, and this influence is inadvertently interpreted as a treatment effect. We deal with the maturation effect with the use of control variables for tenure of users on the platform. Hence, observed patterns in disclosure outcomes as the continuation of the maturation trend that started before the treatment cannot be an alternative interpretation. Third, it is possible to argue that seasonal variations exist in users' use of Facebook, and therefore disclosure patterns of users

fluctuate over time. The possibility of a time or cyclical trend masquerading as a treatment effect is unlikely because we use month FE to remove time-related variation from disclosure outcomes. In fact, a large time-series design, like ours, was shown to be highly effective in ruling out the possibility of alternative interpretations related to time effects and maturity (Cook and Campbell 1979, pp. 210–211). Fourth, our results do not suffer from statistical regression because we consider all Facebook users in the college and thus do not sample users with low or high disclosure patterns only.

Fifth, history is a threat to internal validity when the observed effect in disclosure behavior might be due to an event that takes place during intervention or shortly after intervention. We mitigate the effect of history by using a small window for the short-run analysis. However, by setup, we cannot do the same thing for the long-run analysis. Therefore, to rule out viable alternative explanations in a systematic manner, we perform two checks. We first review the literature on OSN privacy to see if there is any privacy change event related to Facebook in our time frame. We identify another policy change rolled out by Facebook on May 26, 2010 (Tucker 2014). Apart from a simpler privacy settings page for the content users' posts, Facebook announced controls to turn off applications and to limit access to basic profile information (FB News Room 2010). This change appears to be within our long-term window. To make sure that our findings are not biased, we estimate the long-run panel models with an additional event dummy, taking a value of 1 after May 26, 2010, and 0 otherwise. Although the new event dummy corresponding to this event is significant and positive in column (18), the qualitative impact of our main event remains the same. Next, we review the history of Facebook,[23] looking for events or changes that might have influenced users' disclosure behavior. We especially focus on product-related events rather than financial/acquisition events. We find only two such events between the privacy policy change that we study coming into effect (November 9, 2009) and the last week in our data set (May 23, 2011).[24] These events are (i) the introduction of *community pages* around topics like cooking, cycling, and hiking and (ii) the introduction of *instant personalization* with sites like Yelp and Pandora. Facebook users cannot edit community pages, which aggregate content from Wikipedia and users' public wall posts; that is, community pages do not allow for a two-way dialog in the form of user posts or messages. In addition, they do not generate stories in users' news feeds. Therefore, we do not expect to see a change in the disclosure behavior as users have no control over the content of these community pages. To confirm this, we run the long-run models with observations until the introduction of community pages. Our results, reported in column (19), suggest that our results do not change qualitatively. Although we do not count (or include) automatic posts placed by external sites as a result of instant personalization on users' walls in the number of posts, we also estimate the long-run model after excluding the observations in the period of instant personalization. Our findings given in column (20) reveal that our results remain the same. Overall, we conclude that history effects do not provide plausible alternative explanations for the observed change in the content sharing and disclosure behavior of users as a result of the privacy policy change.

7. Discussion

Privacy critics opposed Facebook's change in December 2009 on the grounds of the company having a hidden agenda to promote more openness among Facebook users. We find strong evidence of induced behavior of greater open disclosure after the change. Users, on average, share relatively more content openly than before because they generate more wall posts and fewer private messages. We attribute this change to the increased ability to control shared content: Facebook users fear of privacy loss due to lack of control to limit the audience for their wall posts and the reduction in this fear facilitated by new controls has resulted in the use of wall posts more and the use of private messages less, subsequently increasing the open disclosure of user-generated content. Although privacy groups are partially right in their concerns about higher levels of open disclosure, the resulting impact cannot be generalized to all Facebook users. Even if an average Facebook user displays a propensity to share more content openly after the policy change, our findings imply that the reaction of Facebook users to the change is also a function of their prior disclosure patterns and revealed gender. Specifically, users (i) who choose to reveal their gender and (ii) who broadly share content before the change (i.e., those users who are likely to be less privacy sensitive ex ante, in general) are affected rather differently. These groups of users, in fact, reduced their openness in response to the change. Hence, users who were

[23] See http://en.wikipedia.org/wiki/Timeline_of_Facebook.

[24] In terms of new product features and privacy policy changes, Facebook was quite dormant during the time period that we study. Many changes that might have affected user disclosures, like video calling, Facebook Messenger, Timeline, and several accessibility changes related to mobile devices, were introduced after the end of our study period.

initially less cognizant of privacy were prompted by the change regarding privacy threats and subsequently changed their content-sharing behavior in favor of less open disclosures. On the other hand, (iii) users who do not reveal their gender and (iv) users who have more secret disclosure patterns before the change (i.e., those users who are likely to be more privacy sensitive ex ante, in general) are affected by the change in the same way as an average Facebook user. Hence, users who were initially more conscious of privacy reduced their fear about privacy threats because of new granular privacy controls and subsequently changed their content-sharing behavior in favor of more open disclosures. Overall, our results demonstrate that the privacy change fosters openness (secrecy) in content sharing among users who are more (less) privacy sensitive ex ante. Thus, depicting this change as a vehicle to facilitate greater open disclosure across the board is not a true characterization. However, overall, Facebook has achieved more public sharing of user-generated content. This benefit is in addition to the benefit of addressing the privacy outcry of users regarding the lack of controls in choosing the audience for shared content.

8. Conclusions and Limitations

In this study, we examine the relationship between privacy controls and content-sharing activities and the resulting disclosure patterns of users in the context of the Facebook social network. Our study is based on the exogenous policy change in the platform in December 2009 that introduced more granular privacy controls. New controls enabled users to choose the intended audience for each wall post individually instead of using the same audience for every post. Our results show that Facebook users, on average, *increased* the use of wall posts and *decreased* the use of private messages. Furthermore, based on content-generation activities, the sharing patterns of users have changed to reflect the *increased openness* (or *decreased secrecy*) in disclosure. These behavioral changes not only occurred immediately but also lasted over time. Overall, giving users more control over the reach of wall posts has resulted in more open disclosure of peer-produced content.

Although the privacy policy change is influential in facilitating broader sharing of the content users put out on the platform, there are some nuanced differences in induced reaction to the policy change. Our results highlight the importance of user-specific factors such as prior sharing patterns, size of friendship network, and gender disclosure (or lack thereof) in shaping users' responses to the change. We find that users generate fewer wall posts and more private messages as their friendship network expands. This also leads to a reduction in openness of their disclosures. However, users become less conservative and more open as their network grows after the change. Hence, the policy change is instrumental in mitigating the negative impact of network size on open disclosures, thereby fostering greater public exchange of information among users. We also observe that users who reveal their gender are more active in terms of content sharing and more open in terms of disclosure patterns. However, these users lower their openness and become more private in their disclosures after the change. Finally, we show that, in reaction to the change, users with exclusive prior disclosure patterns increase the use of wall posts and decrease the use of private messages. By contrast, users with inclusive prior disclosure patterns decrease the use of wall posts and increase the use of private messages. Taken together, our results suggest that the variation among *more* privacy sensitive users (those who do not reveal their gender and/or those who have exclusive disclosure patterns ex ante) and *less* privacy sensitive users (those who reveal their gender and/or those who have inclusive disclosure patterns ex ante) diminishes after the change, giving rise to a more homogeneous user base in terms of content-generation activities and disclosure patterns.

To sum up, our results provide strong empirical evidence that Facebook achieved more openness and less secrecy among users in content sharing with the help of the policy change. Overall, open disclosure of shared content on the platform has increased. Hence, users responded to the change by becoming more public in sharing content with their peers. However, some users, especially those who were less privacy sensitive prior to the change, reduced the openness of their disclosures after the change. Thus, characterizing the privacy change event as a means to foster open disclosure across all users does not correctly depict the true influence of the change.

In addition to significant empirical findings, our study contributes to the privacy literature on OSNs in new and important ways. First, for the first time, we characterize disclosure behavior in terms of dynamic content-sharing activities, unlike the prior studies focusing mostly on static profile data. This type of analysis was not possible earlier because of the proprietary nature of data. Second, prior privacy studies on OSNs almost exclusively relied on experimental or survey data to assess the potential impact of a change in privacy policies or privacy controls. Instead of conducting an experiment on or surveying a small group of users, our empirical results originate from unique

observational data from a large social network site. Third, earlier studies often used "intention" to disclose as a dependent variable. However, the privacy paradox suggests that individuals actually disclose more than their reported intentions. In this study, we use the "actual" disclosure behavior and show the relationship between privacy controls and actual disclosure behavior. Fourth, we introduce to the literature a simple but very useful metric, called the disclosure index, to capture the patterns of content-sharing activities of OSN users in relative terms. This index serves as a proxy to characterize disclosure behavior using two popular content-sharing activities with different degrees of openness and secrecy implications. Fifth, our results complement the recent experimental and qualitative findings on the relationship between privacy controls and disclosure of information in user profiles. Changes that give users more control over their personal profile information may have the unintended consequence of eliciting greater disclosure of personal information (Brandimarte et al. 2013, Stutzman et al. 2012). Sixth, we find that privacy controls may help OSN platforms create a more homogeneous user base with respect to privacy sensitivity. Last, our findings shed light on the policy debate surrounding the effectiveness of solutions relying solely on privacy controls for privacy protection of OSN users. We show that privacy controls may not serve as a panacea to privacy protection for everyone.

Although granular controls that limit the audience for wall posts have been very much commended (CNN 2009), the same change has also been criticized on the grounds that it required too many clicks from users to change the recommended settings (Singel 2009). Based on the data from the initial 20 million users who have gone through the "transition tool," Facebook reports that more than half of them have made some changes to recommended settings (Stone 2009). This is very surprising given that only 15%–20% of users had changed their privacy settings in the past (Kirkpatrick 2009). Hence, the users become more proactive than ever before, and the worries of the privacy advocates seem to be mitigated by the modification of the privacy settings by users.[25]

We acknowledge that we use the frequency of different content-sharing activities to characterize the level of openness (or closedness) in the disclosure patterns of users. We do not consider how many people become the recipients of disclosed content. It is possible that Facebook users generate more wall posts after the policy change and yet use the in-line controls extensively to reduce the reach of their wall posts. We do not have data on how often users take advantage of new privacy controls to restrict who can see their wall posts. However, as part of the policy change, Facebook loosened the recommended privacy settings of users who have never edited their settings before from "only friends" to "everyone" for wall posts, leading to an increase in openness by default. Given that some users did not change the new settings for wall posts, Facebook effectively switched these users to share their status updates, links, pictures, and videos with the whole Web (Kirkpatrick 2009). Furthermore, even with in-line controls, wall posts are likely to reach more than one peer and thus are less secret than private messages. Hence, the increase in openness of disclosure we identify in this study in terms of the amount of content-generation activities due to the policy change may well imply an increase in openness of disclosure in terms of the number of recipients of shared content.

Similar to prior studies on information disclosure on social networks, we consider users from a specific college, and our sample may not truly represent a random sample of all Facebook users. Given that our selected college is a medium-sized institution, we do not believe that our sample is necessarily biased. However, readers should still exercise caution when interpreting our results or generalizing them to other social networks.

Notwithstanding these limitations, the present study, which we believe is unique in examining information disclosure practices on social networks through dynamic content-sharing activities, provides useful insights into the value of privacy controls for openness and secrecy of disclosures.

[25] We thank the anonymous reviewer for bringing this point to our attention.

Supplemental Material

Supplemental material to this paper is available at https://doi.org/10.1287/isre.2016.0672.

Acknowledgments

The authors thank Facebook and the Facebook Data Science Team, especially former members Cameron Marlow and Jonathan Chang, for their collaboration, which made this research possible. The authors also thank Alejandro Zentler, Khim-Yong Goh, Eric Zheng, David Godes, and the participants at the Workshop on Information Systems and Economics in Orlando, Florida, the INFORMS Marketing Science Society Conference in Istanbul, Turkey, the Workshop on the Economics of Information Security in Washington, DC, and the Americas Conference on Information Systems in Puerto Rico for their helpful feedback. This research was supported in part by the National Science Foundation [Awards CAREER IIS-1149662 and IIS-1409177], by the Office of Naval Research Young Investigator Program [Award N00014-14-1-0485 to Harvard University], and by the National University of Singapore [Research Grant R-253-000-110-112].

Table A.1 Robustness Checks (Dependent Variable: *Message*)

Model Robustness check	(1) GLS estimator—Base model	(2) GLS estimator—Base model	(3) Weekly policy effect	(4) Clustered errors	(5) Clustered errors	(6) Different window—4 weeks	(7) Different window—8 weeks	(8) Different window—52 weeks	(9) Falsification—6 months	(10) Removing outliers—Content	(11) Removing outliers—Content
AfterPolicy	−0.0276***	−0.0324***		−0.0115***	−0.0134***	−0.0122***	−0.0141***	−0.0124***	0.0019	−0.0058**	−0.0056***
	(0.0027)	(0.0015)		(0.0039)	(0.0038)	(0.0032)	(0.0025)	(0.0015)	(0.0030)	(0.0025)	(0.0014)
OSNAge	−0.0009***	−0.0009***	−0.0011***	−0.0011***	−0.0011***	−0.0011***	−0.0011***	−0.0011***	−0.0008***	−0.0010***	−0.0010***
	(0.0000)	(0.0000)	(0.0000)	(0.0001)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)
*Week*120			−0.0175***								
			(0.0056)								
*Week*121			−0.0310***								
			(0.0056)								
*Week*122			−0.0117**								
			(0.0056)								
*Week*123			−0.0096*								
			(0.0057)								
*Week*124			−0.0163***								
			(0.0057)								
*Week*125			0.0004								
			(0.0057)								
Month effects	Included	Included	Included	Included	Included	Included	Included	Included	Included	Included	Included
Constant	0.4240***	0.4290***	0.4588***	0.4610***	0.4570***	0.4610***	0.4630***	0.4560***	0.4340***	0.4042***	0.4030***
	(0.0043)	(0.0037)	(0.0023)	(0.0059)	(0.0051)	(0.0023)	(0.0022)	(0.0020)	(0.0028)	(0.0021)	(0.0016)
R^2	0.010	0.012	0.452	0.452	0.394	0.454	0.451	0.417	0.473	0.411	0.360
Specification	RE	RE	FE	FE	FE	FE	FE	FE	FE	FE	FE
Analysis	Short run	Long run	Short run	Short run	Long run	Short run	Short run	Long run	Short run	Short run	Long run
Observations	1,535,025	2,428,885	1,535,025	1,535,025	2,428,885	1,508,735	1,561,315	2,139,695	1,219,545	1,508,561	2,384,828
Users	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145

Table A.1 (Continued)

Model	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)
Robustness check	Removing outliers—Friend	Removing outliers—Friend	GLS estimator—Extended model	GLS estimator—Subgroup analysis	Cutoff for subgroup analysis—5%	Cutoff for subgroup analysis—20%	Controlling for another policy change	History effect—Community pages	History effect—Personalization
AfterPolicy	−0.0119***	−0.0140***	0.0906***	0.0917***	0.0715***	0.0733***	−0.0229***	−0.0285***	−0.0293***
	(0.0027)	(0.0015)	(0.0018)	(0.0018)	(0.0018)	(0.0018)	(0.0016)	(0.0019)	(0.0019)
OSNAge	−0.0010***	−0.0010***	−0.0010***	−0.0010***	−0.0008***	−0.0008***	−0.0012***	−0.0011***	−0.0011***
	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)
Top%				0.7210***					
				(0.0085)					
Bottom%				0.3110***					
				(0.0086)					
Top% × AfterPolicy				−0.2630***	−0.1822***	−0.1207***			
				(0.0028)	(0.0036)	(0.0025)			
Bottom% × AfterPolicy				0.0554***	0.1957***	0.1381***			
				(0.0029)	(0.0036)	(0.0025)			
Friend			0.0002***	−0.0002***	−0.0002***	−0.0002***			
			(0.0000)	(0.0000)	(0.0000)	(0.0000)			
Friend × AfterPolicy			−0.0008***	−0.0007***	−0.0007***	−0.0007***			
			(0.0000)	(0.0000)	(0.0000)	(0.0000)			
Male			0.5780***	0.3880***					
			(0.0066)	(0.0064)					
Female			0.6680***	0.5110***					
			(0.0065)	(0.0062)					
Male × AfterPolicy			0.0332***	0.0753***	0.0503***	0.0493***			
			(0.0022)	(0.0022)	(0.0022)	(0.0026)			
Female × AfterPolicy			−0.0494***	−0.0286***	−0.0446***	−0.0544***			
			(0.0021)	(0.0022)	(0.0022)	(0.0025)			
PolicyMay26							0.0263***		
							(0.0015)		
Month effects	Included	Included	Included	Included	Included	Included	Included	Included	Included
Constant	0.4304***	0.4270***	0.0748***	0.0665***	0.4489***	0.4482***	0.4675***	0.4682***	0.4685***
	(0.0022)	(0.0018)	(0.0042)	(0.0038)	(0.0018)	(0.0018)	(0.0019)	(0.0021)	(0.0021)
R^2	0.443	0.441	0.031	0.035	0.408	0.409	0.394	0.442	0.442
Specification	FE	FE	RE	RE	FE	FE	FE	FE	FE
Analysis	Short run	Long run	Long run	Long run	Long run	Long run	Long run	Long run	Long run
Observations	1,519,869	2,385,375	2,428,885	2,428,885	2,428,885	2,428,885	2,428,885	1,705,910	1,719,055
Users	12,918	12,918	13,145	13,145	13,145	13,145	13,145	13,145	13,145

Table A.1 (Continued)

Model	(21)	(22)	(23)	(24)	(25)
Robustness check	Adding year dummies—Base model	Adding year dummies—Extended model	Adding year dummies—Subgroup analysis	Count model	Count model
AfterPolicy	−0.0200***	0.0591***	0.0604***	−0.1215***	−0.1901***
	(0.0036)	(0.0035)	(0.0035)	(0.0029)	(0.0016)
OSNAge	−0.0016***	−0.0024***	−0.0024***	−0.0019***	−0.0017***
	(0.0004)	(0.0003)	(0.0003)	(0.0000)	(0.0000)
Top% × *AfterPolicy*			−0.2570***		
			(0.0028)		
Bottom% × *AfterPolicy*			0.0692***		
			(0.0029)		
Friend		−0.0002***	−0.0002***		
		(0.0000)	(0.0000)		
Friend × *AfterPolicy*		−0.0007***	−0.0007***		
		(0.0000)	(0.0000)		
Male × *AfterPolicy*		0.0452***	0.0859***		
		(0.0022)	(0.0022)		
Female × *AfterPolicy*		−0.0364***	−0.0175***		
		(0.0021)	(0.0022)		
Year 2008	0.0565***	0.1200***	0.1200***		
	(0.0206)	(0.0159)	(0.0158)		
Year 2009	0.0663	0.1830***	0.1840***		
	(0.0410)	(0.0315)	(0.0315)		
Year 2010	0.1150*	0.2870***	0.2870***		
	(0.0611)	(0.0471)	(0.0470)		
Year 2011		0.3840***	0.3840***		
		(0.0629)	(0.0627)		
Month effects	Included	Included	Included	Included	Included
Constant	0.4360***	0.4280***	0.4280***		
	(0.0031)	(0.0022)	(0.0022)		
R^2	0.452	0.406	0.409		
Specification	FE	FE	FE	Poisson	Poisson
Analysis	Short run	Long run	Long run	Short run	Long run
Observations	1,535,025	2,428,885	2,428,885	1,535,025	2,428,885
Users	13,145	13,145	13,145	13,145	13,145

*$p \leq 0.1$; **$p \leq 0.05$; ***$p \leq 0.01$.

Table A.2 Robustness Checks (Dependent Variable: *Post*)

Model Robustness check	(1) GLS estimator—Base model	(2) GLS estimator—Base model	(3) Weekly policy effect	(4) Clustered errors	(5) Clustered errors	(6) Different window—4 weeks	(7) Different window—8 weeks	(8) Different window—52 weeks	(9) Falsification—6 months	(10) Removing outliers—Content	(11) Removing outliers—Content
AfterPolicy	0.0153***	0.0271***		0.0297***	0.0419***	0.0239***	0.0286***	0.0546***	0.0041	0.0254***	0.0340***
	(0.0024)	(0.0013)		(0.0033)	(0.0032)	(0.0027)	(0.0021)	(0.0013)	(0.0026)	(0.0022)	(0.0012)
OSNAge	−0.0025***	−0.0021***	−0.0027***	−0.0027***	−0.0023***	−0.0027***	−0.0027***	−0.0027***	−0.0026***	−0.0024***	−0.0020***
	(0.0000)	(0.0000)	(0.0000)	(0.0001)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)
*Week*120			0.0318***								
			(0.0048)								
*Week*121			−0.0007								
			(0.0048)								
*Week*122			0.0194***								
			(0.0048)								
*Week*123			0.0434***								
			(0.0049)								
*Week*124			0.0381***								
			(0.0049)								
*Week*125			0.0500***								
			(0.0049)								
Month effects	Included	Included	Included	Included	Included	Included	Included	Included	Included	Included	Included
Constant	0.6880***	0.6540***	0.7299***	0.7340***	0.6830***	0.7320***	0.7340***	0.7087***	0.7281***	0.6618***	0.6192***
	(0.0048)	(0.0042)	(0.0020)	(0.0059)	(0.0054)	(0.0020)	(0.0019)	(0.0017)	(0.0024)	(0.0018)	(0.0014)
R^2	0.031	0.046	0.620	0.620	0.575	0.621	0.619	0.588	0.641	0.593	0.553
Specification	RE	RE	FE	FE	FE	FE	FE	FE	FE	FE	FE
Analysis	Short run	Long run	Short run	Short run	Long run	Short run	Short run	Long run	Short run	Short run	Long run
Observations	1,535,025	2,428,885	1,535,025	1,535,025	2,428,885	1,508,735	1,561,315	2,139,695	1,219,545	1,508,561	2,428,885
Users	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145

Table A.2 (Continued)

Model	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)
Robustness check	Removing outliers—Friend	Removing outliers—Friend	GLS estimator—Extended model	GLS estimator—Subgroup analysis	Cutoff for subgroup analysis—5%	Cutoff for subgroup analysis—20%	Controlling for another policy change	History effect—Community pages	History effect—Personalization
AfterPolicy	0.0271***	0.0388***	0.1600***	0.1610***	0.1418***	0.1411***	0.0024*	0.0151***	0.0147***
	(0.0023)	(0.0013)	(0.0015)	(0.0015)	(0.0015)	(0.0015)	(0.0013)	(0.0016)	(0.0016)
OSNAge	−0.0026***	−0.0022***	−0.0018***	−0.0018***	−0.0016***	−0.0016***	−0.0027***	−0.0028***	−0.0028***
	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)
Top%				0.1800***					
				(0.0085)					
Bottom%				1.1390***					
				(0.0086)					
Top% × AfterPolicy				0.0102***	0.1375***	0.0554***			
				(0.0023)	(0.0030)	(0.0021)			
Bottom% × AfterPolicy				−0.2660***	−0.0321***	−0.0716***			
				(0.0024)	(0.0030)	(0.0021)			
Friend			−0.0004***	−0.0004***	−0.0008***	−0.0008***			
			(0.0000)	(0.0000)	(0.0000)	(0.0000)			
Friend × AfterPolicy			−0.0005***	−0.0004***	−0.0004***	−0.0004***			
			(0.0000)	(0.0000)	(0.0000)	(0.0000)			
Male			0.8500***	0.6510***					
			(0.0070)	(0.0064)					
Female			1.0320***	0.7780***					
			(0.0069)	(0.0062)					
Male × AfterPolicy			−0.1100***	−0.1060***	−0.1134***	−0.0979***			
			(0.0018)	(0.0019)	(0.0019)	(0.0022)			
Female × AfterPolicy			−0.1270***	−0.1060***	−0.1199***	−0.1030***			
			(0.0018)	(0.0018)	(0.0018)	(0.0021)			
PolicyMay26							0.1089***		
							(0.0012)		
Month effects	Included	Included	Included	Included	Included	Included	Included	Included	Included
Constant	0.6911***	0.6436***	0.1370***	0.1280***	0.6935***	0.6937***	0.7278***	0.7400***	0.7403***
	(0.0019)	(0.0015)	(0.0044)	(0.0015)	(0.0015)	(0.0015)	(0.0016)	(0.0018)	(0.0018)
R^2	0.609	0.564	0.081	0.086	0.592	0.592	0.577	0.610	0.609
Specification	FE	FE	RE	RE	FE	FE	FE	FE	FE
Analysis	Short run	Long run	Long run	Long run	Long run	Long run	Long run	Long run	Long run
Observations	1,519,869	2,385,375	2,428,885	2,428,885	2,428,885	2,428,885	2,428,885	1,705,910	1,719,055
Users	12,918	12,918	13,145	13,145	13,145	13,145	13,145	13,145	13,145

Table A.2 (Continued)

Model	(21)	(22)	(23)	(24)	(25)
Robustness check	Adding year dummies—Base model	Adding year dummies—Extended model	Adding year dummies—Subgroup analysis	Count model	Count model
AfterPolicy	0.0156***	0.1070***	0.0110***	0.0338***	0.0551***
	(0.0031)	(0.0030)	(0.0029)	(0.0030)	(0.0017)
OSNAge	−0.0012***	−0.0011***	−0.0011***	−0.0055***	−0.0049***
	(0.0003)	(0.0003)	(0.0003)	(0.0000)	(0.0000)
Top% × *AfterPolicy*			0.0174***		
			(0.0023)		
Bottom% × *AfterPolicy*			−0.2500***		
			(0.0024)		
Friend		−0.0007***	−0.0007***		
		(0.0000)	(0.0000)		
Friend × *AfterPolicy*		−0.0952***	−0.0003***		
		(0.0018)	(0.0000)		
Male × *AfterPolicy*		0.0452***	−0.0924***		
		(0.0022)	(0.0019)		
Female × *AfterPolicy*		−0.1120***	−0.0920***		
		(0.0018)	(0.0018)		
Year 2008	−0.0812***	−0.0360***	−0.0351***		
	(0.0177)	(0.0133)	(0.0133)		
Year 2009	−0.1620***	−0.0953***	−0.0931***		
	(0.0352)	(0.0265)	(0.0264)		
Year 2010	−0.2140***	−0.0856**	−0.0837**		
	(0.0525)	(0.0396)	(0.0395)		
Year 2011		−0.0464	−0.0449		
		(0.0528)	(0.0526)		
Month effects	Included	Included	Included	Included	Included
Constant	0.7230***	0.6930***	0.6930***		
	(0.0027)	(0.0019)	(0.0019)		
R^2	0.620	0.592	0.594		
Specification	FE	FE	FE	Poisson	Poisson
Analysis	Short run	Long run	Long run	Short run	Long run
Observations	1,535,025	2,428,885	2,428,885	1,535,025	2,428,885
Users	13,145	13,145	13,145	13,145	13,145

*$p \leq 0.1$; **$p \leq 0.05$; ***$p \leq 0.01$.

Table A.3 Robustness Checks (Dependent Variable: *Disclosure Index***)**

Model Robustness check	(1) GLS estimator—Base model	(2) GLS estimator—Base model	(3) Weekly policy effect	(4) Clustered errors	(5) Clustered errors	(6) Different window—4 weeks	(7) Different window—8 weeks	(8) Different window—52 weeks	(9) Falsification—6 months	(10) Removing outliers—Content	(11) Removing outliers—Content
AfterPolicy	0.0225***	0.0385***		0.0412***	0.0553***	0.0361***	0.0427***	0.0670***	0.0060	0.0312***	0.0396***
	(0.0031)	(0.0017)		(0.0042)	(0.0035)	(0.0036)	(0.0028)	(0.0017)	(0.0048)	(0.0030)	(0.0016)
OSNAge	−0.0014***	−0.0010***	−0.0016***	−0.0016***	−0.0012***	−0.0016***	−0.0016***	−0.0016***	−0.0019***	−0.0014***	−0.0011***
	(0.0000)	(0.0000)	(0.0000)	(0.0001)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)
*Week*120			0.0494***								
			(0.0065)								
*Week*121			0.0304***								
			(0.0065)								
*Week*122			0.0311***								
			(0.0065)								
*Week*123			0.0337***								
			(0.0066)								
*Week*124			0.0544***								
			(0.0066)								
*Week*125			0.0496***								
			(0.0066)								
Month effects	Included	Included	Included	Included	Included	Included	Included	Included	Included	Included	Included
Constant	0.2420***	0.2070***	0.2711***	0.2720***	0.2260***	0.2710***	0.2720***	0.2528***	0.2941***	0.2576***	0.2162***
	(0.0039)	(0.0034)	(0.0027)	(0.0055)	(0.0047)	(0.0026)	(0.0025)	(0.0022)	(0.0033)	(0.0024)	(0.0019)
R^2	0.007	0.006	0.224	0.224	0.193	0.225	0.224	0.204	0.238	0.210	0.183
Specification	RE	RE	FE	FE	FE	FE	FE	FE	FE	FE	FE
Analysis	Short run	Long run	Short run	Short run	Long run	Short run	Short run	Long run	Short run	Short run	Long run
Observations	1,535,025	2,428,885	1,535,025	1,535,025	2,428,885	1,508,735	1,561,315	2,139,695	1,219,545	1,508,561	2,428,885
Users	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145	13,145

Table A.3 (Continued)

Model	(12)	(13)	(14)	(15)	(16)	(17)	(18)	(19)	(20)
Robustness check	Removing outliers—Friend	Removing outliers—Friend	GLS estimator—Extended model	GLS estimator—Subgroup analysis	Cutoff for subgroup analysis—5%	Cutoff for subgroup analysis—20%	Controlling for another policy change	History effect—Community pages	History effect—Personalization
AfterPolicy	0.0390***	0.0529***	0.0794***	0.0715***	0.0703***	0.0678***	0.0253***	0.0436***	0.0440***
	(0.0031)	(0.0017)	(0.0020)	(0.0019)	(0.0021)	(0.0021)	(0.0018)	(0.0022)	(0.0021)
OSNAge	−0.0016***	−0.0012***	−0.0009***	−0.0008***	−0.0008***	−0.0008***	−0.0015***	−0.0016***	−0.0016***
	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)	(0.0000)
Top%				−0.5600***					
				(0.0057)					
Bottom%				0.7920***					
				(0.0058)					
Top% × AfterPolicy				0.2690***	0.3197***	0.1761***			
				(0.0032)	(0.0042)	(0.0029)			
Bottom% × AfterPolicy				−0.3300***	−0.2278***	−0.2097***			
				(0.0033)	(0.0041)	(0.0029)			
Friend			−0.0003***	−0.0003***	−0.0006***	−0.0006***			
			(0.0000)	(0.0000)	(0.0000)	(0.0000)			
Friend × AfterPolicy			0.0002***	0.0003***	0.0003***	0.0003***			
			(0.0000)	(0.0000)	(0.0000)	(0.0000)			
Male			0.2410***	0.2300***					
			(0.0067)	(0.0044)					
Female			0.3330***	0.2370***					
			(0.0065)	(0.0043)					
Male × AfterPolicy			−0.1510***	−0.1900***	−0.1637***	−0.1472***			
			(0.0025)	(0.0025)	(0.0026)	(0.0030)			
Female × AfterPolicy			−0.0858***	−0.0861***	−0.0753***	−0.0486***			
			(0.0025)	(0.0025)	(0.0025)	(0.0029)			
PolicyMay26							0.0826***		
							(0.0017)		
Month effects	Included	Included	Included	Included	Included	Included	Included	Included	Included
Constant	0.2607***	0.2167***	0.0666***	0.0632***	0.2445***	0.2454***	0.2603***	0.2718***	0.2718***
	(0.0025)	(0.0020)	(0.0043)	(0.0029)	(0.0021)	(0.0021)	(0.0022)	(0.0024)	(0.0024)
R^2	0.223	0.191	0.008	0.017	0.199	0.202	0.194	0.219	0.218
Specification	FE	FE	RE	RE	FE	FE	FE	FE	FE
Analysis	Short run	Long run	Long run	Long run	Long run	Long run	Long run	Long run	Long run
Observations	1,519,869	2,385,375	2,428,885	2,428,885	2,428,885	2,428,885	2,428,885	1,705,910	1,719,055
Users	12,918	12,918	13,145	13,145	13,145	13,145	13,145	13,145	13,145

Table A.3 (Continued)

Model	(21)	(22)	(23)
Robustness check	Adding year dummies—Base model	Adding year dummies—Extended model	Adding year dummies—Subgroup analysis
AfterPolicy	0.0357***	0.0477***	0.0498***
	(0.0042)	(0.0041)	(0.0040)
OSNAge	0.0004	0.0014***	0.0013***
	(0.0005)	(0.0003)	(0.0003)
Top% × *AfterPolicy*			0.2740***
			(0.0032)
Bottom% × *AfterPolicy*			−0.3200***
			(0.0033)
Friend		−0.0005***	−0.0005***
		(0.0000)	(0.0000)
Friend × *AfterPolicy*		0.0002***	0.0003***
		(0.0000)	(0.0000)
Male × *AfterPolicy*		−0.1400***	−0.1780***
		(0.0025)	(0.0026)
Female × *AfterPolicy*		−0.0752***	−0.0745***
		(0.0025)	(0.0025)
Year 2008	−0.1380***	−0.1560***	−0.1550***
	(0.0238)	(0.0183)	(0.0182)
Year 2009	−0.2290***	−0.2780***	−0.2770***
	(0.0473)	(0.0364)	(0.0363)
Year 2010	−0.3290***	−0.3720***	−0.3710***
	(0.0705)	(0.0544)	(0.0542)
Year 2011		−0.4300***	−0.4290***
		(0.0726)	(0.0723)
Month effects	Included	Included	Included
Constant	0.2870***	0.2650***	0.2650***
	(0.0036)	(0.0026)	(0.0026)
R^2	0.224	0.196	0.203
Specification	FE	FE	FE
Analysis	Short run	Long run	Long run
Observations	1,535,025	2,428,885	2,428,885
Users	13,145	13,145	13,145

***$p \leq 0.01$.

References

Acquisti A, Gross R (2006) Imagined communities: Awareness, information sharing, and privacy on the Facebook. Danezis G, Golle P, eds. *6th Workshop Privacy Enhancing Tech.*, Lecture Notes Comput. Sci., Vol. 4258 (Springer-Verlag, Berlin Heidelberg), 36–58.

Airoldi EM, Rubin DB (2017) Some fundamental ideas for causal inference on networks. *Proc. Natl. Acad. Sci. USA* Forthcoming.

Altman I (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding* (Brooks/Cole, Monterey, CA).

Anderson CL, Agarwal R (2011) The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Inform. Systems Res.* 22(3):469–490.

Anderson K (2010) Is Facebook eroding privacy? Or does social media require us to lower our expectations? *The Scholarly Kitchen* (May 10). https://scholarlykitchen.sspnet.org/2010/05/10/is-facebook-eroding-privacy-or-does-social-media-require-us-to-lower-our-expectations/.

Awad NF, Krishnan MS (2006) The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quart.* 30(1):13–28.

Bankston K (2009) Facebook's new privacy changes: The good, the bad, and the ugly. *EFF* (December 9). https://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly.

Bélanger F, Crossler RE (2011) Privacy in the digital age: A review of information privacy research in information systems. *MIS Quart.* 35(4):1017–1042.

Berman JJ, Meyer J, Coats G (1984) Effects of program characteristics on treatment outcome: An interrupted time-series analysis. *J. Stud. Alcohol* 45(5):405–410.

boyd DM, Hargittai E (2010) Facebook privacy settings: Who cares? *First Monday* 15(8). http://firstmonday.org/article/view/3086/2589.

Brandimarte L, Acquisti A, Loewenstein G (2013) Misplaced confidences: Privacy and the control paradox. *Soc. Psych. Personality Sci.* 4(3):340–347.

Caverlee J, Webb S (2008) A large-scale study of Myspace: Observations and implications for online social networks. *Internat. Conf. Weblogs Soc. Media* (AAAI, Palo Alto, CA).

Chellappa R, Sin R (2005) Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Inform. Tech. Management* 6:181–202.

Chen X, van der Lans R, Phan TQ (2016) Uncovering the importance of relationship characteristics in social networks: Implications for seeding strategies. *J. Marketing Res.* Forthcoming.

Cheng J (2009) An updated guide to Facebook privacy: December 2009 edition. *Ars Technica* (December 27). http://arstechnica.com/business/2009/12/an-updated-guide-to-facebook-privacy-december-2009-edition/.

CNN (2009) Facebook unveils privacy changes. (December 10), http://www.cnn.com/2009/TECH/12/10/facebook.privacy/.

Coates TJ, Jeffery RW, Slinkard LA (1981) Heart healthy eating and exercise: Introducing and maintaining changes in health behaviors. *Amer. J. Public Health* 71(1):15–23.

Coburn AF, Fortinsky R, McGuire C, McDonald TP (1993) Effect of prospective reimbursement on nursing home costs. *Health Services Res.* 28(1):45–68.

Community Tool Box (2014) Selecting an appropriate design for the evaluation. http://ctb.ku.edu/en/table-of-contents/evaluate/evaluate-community-interventions/experimental-design/main.

Cook TD, Campbell DT (1979) *Quasi-Experimentation: Design and Analysis Issues for Field Settings* (Houghton Mifflin, Boston).

Culnan M, Armstrong P (1999) Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organ. Sci.* 10(1):104–115.

Dey R, Jelveh Z, Ross K (2012) Facebook users have become much more private. *IEEE Internat. Conf. Pervasive Comput. Comm. Workshops* (IEEE Computer Society, Washington, DC), 346–352.

Dinev T, Hart P (2006) An extended privacy calculus model for e-commerce transactions. *Inform. Systems Res.* 17(1):61–80.

Dinev T, Bellotto M, Hart P, Russo V, Serra I, Colautti C (2006) Privacy calculus model in e-commerce—A study of Italy and the United States. *Eur. J. Inform. Systems* 15(4):389–402.

Donath J, boyd D (2004) Public displays of connection. *BT Tech. J.* 22(4):71–82.

Electronic Privacy Information Center (2013) Social networking privacy. http://epic.org/privacy/socialnet/.

Emerson RM (1976) Social exchange theory. *Annual Rev. Sociol.* 2: 335–362.

Facebook (2015) Facebook reports third quarter 2015 results. Report, Press release, https://investor.fb.com/investor-news/press-release-details/2015/Facebook-Reports-Third-Quarter-2015-Results/.

FB News Room (2010) Facebook redesigns privacy. (May 26). https://newsroom.fb.com/news/2010/05/facebook-redesigns-privacy/.

Fischhoff B, Slovic P, Lichtenstein S, Read S, Combs B (1978) How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy Sci.* 8:127–152.

Forastiere L, Airoldi EM, Mealli F (2016) Identification and estimation of treatment and interference effects in observational studies on networks. Arxiv/Stat.ME. 1609.06245. https://arxiv.org/abs/1609.06245.

Freeman K (2012) Facebook privacy: This service alerts you when it changes [INFOGRAPHIC]. *Mashable* (May 14), http://mashable.com/2012/05/14/privacywatch-infographic/.

Gillings D, Makuc D, Siegel E (1981) Analysis of interrupted time series mortality trends: An example to evaluate regionalized perinatal care. *Amer. J. Public Health* 71:38–46.

Glass GV (1997) Interrupted time-series quasi-experiments. Jaeger RM, ed. *Complementary Methods for Research in Education*, 2nd ed. (American Educational Research Association, Washington, DC), 589–609.

Gottlieb JD, Townsend RR, Xu T (2016) Experimenting with entrepreneurship: The effect of job-protected leave. Tuck School of Business Working Paper 2714577, Dartmouth College, Hanover, NH.

Gross R, Acquisti A (2005) Information revelation and privacy in online social network (the Facebook case). *ACM Workshop Privacy Electronic Soc.* (ACM, New York), 71–80.

Hann IH, Hui KL, Lee SYT, Png IPL (2007) Overcoming online information privacy concerns: An information-processing theory approach. *J. Management Inform. Systems* 24(2):13–42.

Hoadley CM, Xu H, Lee JJ, Rosson MB (2010) Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry. *Electronic Commerce Res. Appl.* 9(1): 50–60.

Johnson B, Christensen L (2010) *Educational Research: Quantitative, Qualitative, and Mixed Approaches*, 4th ed. (Sage, Thousand Oaks, CA).

Jones H, Soltren JH (2005) Facebook: Threats to privacy. Working paper, Massachusetts Institute of Technology, Cambridge, http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf.

Kincaid J (2009) The Facebook privacy fiasco begins. *TechCrunch* (December 9), http://techcrunch.com/2009/12/09/facebook-privacy/.

Kirkpatrick M (2009) Why Facebook changed its privacy strategy. *ReadWrite* (December 10). http://readwrite.com/2009/12/10/why_facebook_changed_privacy_policies/.

Klopfer PH, Rubenstein DI (1977) The concept privacy and its biological basis. *J. Soc. Issues* 33(3):52–65.

Korth A (2012) On privacy in social networks: The provider's perspective. *ReadWrite* (May 7), http://readwrite.com/2012/05/07/on-privacy-in-social-networks-the-providers-perspective.

Krasnova HS, Koroleva K, Hildebrand T (2010) Online social networks: Why we disclose. *J. Inform. Tech.* 25(2):109–125.

Lampe C, Ellison NB, Steineld C (2006) A face(book) in the crowd: Social searching vs. social browsing. *Proc. ACM Conf. Comput. Supported Cooperative Work* (ACM, New York), 167–170.

Lampinen A, Tamminen S, Oulasvirta A (2006) All my people right here, right now: Management of group co-presence on a social networking site. *Proc. ACM 2009 Internat. Conf. Supporting Group Work* (ACM, New York), 281–290.

Lampinen A, Lehtinen V, Lehmuskallio A, Tamminen S (2011) We're in it together: Interpersonal management of disclosure in social network services. *Proc. 2011 Annual Conf. Human Factors Comput. Systems* (ACM, New York), 3217–3226.

Langer EJ (1975) The illusion of control. *J. Personality Soc. Psych.* 32(2):311–328.

Laufer RS, Wolfe M (1977) Privacy as a concept and a social issue—Multidimensional developmental theory. *J. Soc. Issues* 33: 22–42.

Lee DS, Lemieux T (2010) Regression discontinuity designs in economics. *J. Econom. Literature* 48(2):281–355.

Lewis K (2011) The co-evolution of social network ties and online privacy behaviour. Trepte S, Reinecke L, eds. *Privacy Online* (Springer-Verlag, Berlin Heidelberg), 91–109.

Lewis K, Kaufman J, Christakis N (2008) The taste for privacy: An analysis of college student privacy settings in an online social network. *J. Comput.-Mediated Comm.* 14(1):79–100.

Malhotra NK, Kim SS, Agarwal J (2004) Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Inform. Systems Res.* 15(4):336–355.

Margulis ST (2003) Privacy as a social issue and behavioral concept. *J. Soc. Issues* 59:243–261.

Marwick AE, boyd DM (2011) I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media Soc.* 13(1):114–133.

Michielutte R, Shelton B, Paskett ED, Tatum CM, Velez R (2000) Use of an interrupted time-series design to evaluate a cancer screening program. *Health Educ. Res.* 15(5):615–623.

Milberg SJ, Burke SJ, Smith HJ, Kallman EA (1995) Values, personal information privacy, and regulatory approaches. *Comm. ACM* 38(12):65–74.

Naone E (2010) The changing nature of privacy on Facebook. *MIT Tech. Rev.* (May 3), https://www.technologyreview.com/s/418766/the-changing-nature-of-privacy-on-facebook/.

Opshal K (2010) Facebook's eroding privacy policy: A timeline. *EFF* (April 28), https://www.eff.org/deeplinks/2010/04/facebook-timeline/.

Peltzman S (1975) The effects of automobile safety regulation. *J. Political Econom.* 83:677–726.

Petronio S (1999) Preface: The meaning of balance. Petronio S, ed. *Balancing the Secrets of Private Disclosures* (Psychology Press, New York), xiii–xvi.

Petronio SS (2002) *Boundaries of Privacy: Dialectics of Disclosure* (SUNY Press, Albany, NY).

Phan TQ, Airoldi EM (2015) A natural experiment of social network formation and dynamics. *Proc. Natl. Acad. Sci. USA* 112(21): 6595–6600.

Posner RA (1981) The economics of privacy. *Amer. Econom. Rev.* 71(2):405–409.
Ross HL, Campbell DT, Glass GV (1970) Determining the social effects of a legal reform. Nagel SS, ed. *Law and Social Change* (Sage, Beverly Hills, CA), 15–32.
Sanghvi R (2009) New tools to control your experience. *Facebook* (December 9). https://www.facebook.com/notes/facebook/new-tools-to-control-your-experience/196629387130/.
Singel R (2009) Public posting now the default on Facebook. *Wired* (December 9), http://www.wired.com/2009/12/facebook-privacy-update/.
Smith HJ, Dinev T, Xu H (2011) Information privacy research: An interdisciplinary review. *MIS Quart.* 35(4):989–1016.
Smith HJ, Milberg SJ, Burke SJ (1996) Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quart.* 20(2):167–196.
Stone B (2009) Facebook's privacy changes draw more scrutiny. *New York Times* (December 10), http://bits.blogs.nytimes.com/2009/12/10/facebooks-privacy-changes-draw-more-scrutiny/.
Stutzman F (2006) An evaluation of identity-sharing behavior in social network communities. *Internat. Digital Media Arts J.* 3(1):10–18.
Stutzman F, Gross R, Acquisti A (2012) Silent listeners: The evolution of privacy and disclosure on Facebook. *J. Privacy Confidentiality* 4(2):7–41.
Stutzman FD, Duffield JK (2010) Friends only: Examining a privacy-enhancing behavior in Facebook. *Inter. Conf. Human Factors Comput. Systems* (ACM, New York), 1553–1562.
Thelwall M (2008) Social networks, gender and friending: An analysis of Myspace member profiles. *J. Amer. Soc. Inform. Sci. Tech.* 59(8):1321–1330.
Thompson SC (1999) Illusions of control: How we overestimate our personal influence. *Current Directions Psych. Sci.* 8(6):187–190.
Tucker C (2014) Social networks, personalized advertising, and privacy controls. *J. Marketing Res.* 51(5):546–562.
Tufekci Z (2008) Can you see me now? Audience and disclosure regulation in online social network sites. *Bull. Sci. Tech. Soc.* 28(1):20–36.
Vroom VH (1964) *Work and Motivation* (Wiley, New York).
Williams D (2012) How Facebook's 'frictionless sharing' can create better ads on Facebook. *AdvertisingAge* (January 30), http://adage.com/article/digitalnext/facebook-s-frictionless-sharing-create-ads-facebook/232419/.
Xu H (2007) The effects of self-construal and perceived control on privacy concerns. *Internat. Conf. Inform. Systems* (AIS, Atlanta), 1–14.
Xu H, Teo HH, Tan BCY, Agarwal R (2009) The role of push–pull technology in privacy calculus: The case of location-based services. *J. Management Inform. Systems* 26(3):135–173.