"We Are the Product": Public Reactions to Online Data Sharing and Privacy Controversies in the Media

Casey Fiesler
Department of Information Science
University of Colorado Boulder
casey.fiesler@colorado.edu

Blake Hallinan
Department of Communication
University of Colorado Boulder
blake.hallinan@colorado.edu

ABSTRACT
As online platforms increasingly collect large amounts of data about their users, there has been growing public concern about privacy around issues such as data sharing. Controversies around practices perceived as surprising or even unethical often highlight patterns of privacy attitudes when they spark conversation in the media. This paper examines public reaction "in the wild" to two data sharing controversies that were the focus of media attention—regarding the social media and communication services Facebook and WhatsApp, as well as the email service unroll.me. These controversies instigated discussion of data privacy and ethics, accessibility of website policies, notions of responsibility for privacy, cost-benefit analyses, and strategies for privacy management such as non-use. An analysis of reactions and interactions captured by comments on news articles not only reveals information about pervasive privacy attitudes, but also suggests communication and design strategies that could benefit both platforms and users.

Author Keywords
data; data sharing; ethics; journalism; non-use; online comments; online platforms; policy; privacy; social media; terms of service

ACM Classification Keywords
K.4.1 Computers and Society: Public Policy Issues—Privacy

INTRODUCTION
As online platforms increasingly collect large amounts of data about their users, there has been growing public concern around issues of data privacy. This is a particularly complex problem space for technology designers due to the potentially competing interests of users and market forces that drive business models [30].

CHI 2018, April 21–26, 2018, Montreal, QC, Canada

ACM 978-1-4503-5620-6/18/04…$15.00
https://doi.org/10.1145/3173574.3173627

Consumers have long expressed concern about how their data is used, particularly with respect to monetization or data sharing with third parties [18,40]. However, the shift of much of our lives online, from commerce to socializing, has created new perceived privacy threats beyond telemarketer call lists and shopper loyalty cards. This new landscape of digital privacy also creates complex interaction design problems, as people often express attitudes towards privacy that are not reflected in their behavior [1].

Understanding user attitudes towards privacy, particularly in the context of specific technologies such as social media [1,53] or mobile apps [26,31,44], has been an important area of research. It has also led to interventions such as usable privacy policies [25] or design recommendations [3,30]. This research is motivated in part by the knowledge that online privacy continues to pose challenges for the general public as they navigate technology use online.

We often see evidence of these challenges in the form of public outrage to privacy controversies. Two recent examples of a type of privacy violation—data being shared with or sold to third parties—include (1) the messenger app WhatsApp altering its policies to include data sharing with Facebook, and (2) the email service unroll.me selling anonymized data to Uber. Though much social media privacy research has been concerned with privacy concerns around known individuals rather than "faceless third parties" [28], the potential for data to be shared or sold outside of its original context is an issue that cuts across social media, messaging, email, and other online activities.

For this study, we examined user attitudes "in the wild" by analyzing public reactions to these specific controversies, as represented by comments to news articles. This source of data provides not only authentic reactions to real situations (compared to, for example, asking directly about privacy attitudes as part of a research study), but it also touches on an important aspect of public attitudes: how they might be shaped by the media. We know that media portrayals can have a significant influence on attitudes [34,51], particularly when it comes to science [5,27]. As Vines et al. point out in their analysis of public reactions to media portrayals of HCI research, these reactions can reveal tensions around wider

societal issues regarding technology that might be hidden when using traditional user-centered research methods [49].

Our analysis was driven by a set of exploratory research questions: What are the patterns of public reaction to online data sharing controversies? How do in-the-moment reactions track to existing knowledge about privacy attitudes? What are the major points of disagreement in the user community, and do these reflect underlying value differences? What solutions or strategies do commenters suggest in response to perceived privacy violations?

We found that though the majority of articles in our dataset had a negative framing towards each data sharing controversy, the attitudes expressed by commenters were more nuanced than simply being negative towards the platforms. Instead, for the commenters in our dataset, a major determinant for both level of privacy concern and proposed solutions were pre-existing notions for who bears the responsibility for privacy protection—the user or the platform. We conclude with a discussion of the potential effectiveness of proposed solutions, with a focus on accessible and transparent privacy information.

BACKGROUND

In recent years there have been a number of privacy-related uproars heavily covered in the media, many of which relate to major tech companies such as Facebook and Google. Prominent examples include Google Buzz, which seeded a social networking site with email contacts, and the Facebook Beacon product that tracked web activity and then shared it with Facebook friends. These controversies illustrated how problematic expectation violations and feelings of a loss of control can be when it comes to how online platforms use our data [13].

The current study examines two recent controversies that specifically concern these kinds of expectation violations, in the context of companies sharing of data with third parties. Though there is a great deal of prior work uncovering attitudes about online privacy, examining immediate public reactions to specific situations allows us to see how these attitudes manifest in a real world context.

The first controversy concerned the messaging app WhatsApp, which was acquired by Facebook in 2014 but seemingly did not institute major changes following that acquisition [12]. However, in August 2016, WhatsApp announced changes to its privacy policy that specified they would be sharing data with Facebook, stating that Facebook would be using WhatsApp account information to improve ads and user experience. Media coverage of the change was predominantly negative, with many articles offering instructions for opting out of the new terms. There have been subsequent developments in this situation, including a lawsuit in India, but this study concerns the initial public reaction to the announcement of the policy change.

The second controversy involved unroll.me, a service that gives users the ability to see a list of all of their email subscriptions and to easily unsubscribe. To accomplish this, the service requires access to the user's email account. Unroll.me is owned by Slice Technologies, a company with market research services that extracts and analyzes information from commercial emails. In April 2017, a *New York Times* expose on Uber's business practices revealed that they purchased data from unroll.me about the content of receipts from Lyft, their major competitor [23]. This revelation was met with surprise by unroll.me users, and journalists picked up this piece of the story and ran with it, investigating unroll.me's privacy practices. The CEO of unroll.me released a public statement emphasizing that the practice of selling anonymized data had always been part of their business model and laid out in their privacy policy, noting that "while we try our best to be open about our business model, recent customer feedback tells me we weren't explicit enough" [20].

What these two situations have in common are the media attention and subsequent public reactions to the revelation that personal data in an online service was or would be shared with a third party. They provide concrete examples of the kinds of perceived privacy violations that research has shown impacts attitudes about online privacy.

Related Work

Research has revealed concerns about data privacy since before widespread use of the Internet, though the increase in available data, both knowingly and unknowingly shared, has subsequently exacerbated existing tensions. An early social media privacy study showed that participants ranked privacy concerns extremely highly compared to other societal issues—though there was little relationship between the privacy attitudes reported and how much information they chose to reveal [1]. In other words, people are likely to express more concern than is reflected in their actual behavior. Acquisti put forth that this attitude-behavior gap would not be solved with better privacy technology or increased awareness because it reflects underlying behavioral mechanisms related to self-control and instant gratification [1]. However, others have noted that the "privacy paradox" is not simply a matter of not caring enough to change their behavior. Many users simply feel that they have no control over how their data is used, resulting in a feeling of learned helplessness [44]. Similarly, Hargittai and Marwick found that young people often have a sense of cynicism around online privacy, believing that violations are simply inevitable [19]

However, unpredictability with regard to how people manage their privacy does create challenges, for both technology designers and policymakers attempting to create regulations about personal identity data [10]. For example, would users be willing to switch from one service to another due to privacy concerns? Schreiner et al. conducted a study where they considered the factors that would affect users switching from WhatsApp to another messaging app (Threema) that is known for having strong privacy and security protections [42]. They found that though good privacy protection can be

a pull to bring in new users, dissatisfaction with privacy practices is a stronger effect in pushing users to leave. However, despite this, it was most common that users would *not* be willing to switch, largely due to social cost and inconvenience.

Likewise, prior research has shown that people are willing to trade privacy for convenience [1,42]. Even as people feel negatively about companies that collect too much data, early studies of consumer privacy showed that nevertheless people agreed that targeted advertisements seeded by more available data could be useful [18,40]. Additionally, the benefits of services such as social media are important enough that people are unwilling to pay the "cost" of quitting to protect their privacy [43,37].

Therefore, a common way of conceptualizing privacy within the social computing research community is as a set of trade-offs between risk and benefit [53]. However, this landscape is more nuanced, particularly since privacy norms differ from context to context [37]. Wisniewski et al. put forth the benefits of designing for "privacy fit" to account for unique attitudes and needs, rather than the assumption that more privacy is always better [53]. Different users or stakeholders on the same platform might have different values around privacy that result in tension [36]. Users might be willing or even interested in providing some kinds of information but not others or information for certain uses. For example, the *purpose* of the use has been shown to be particularly important when users have access to that information [43], as well as the scope of use or data retention policies [29]. The type of information being shared also has an impact on attitude [29].

Likewise, prior work shows that even when people see the benefit of a company *itself* having more data about them, attitudes can become strongly negative when that data is shared with third parties [18]. Many consumers would rather see their data used directly for improving the services they are being offered in exchange, rather than commercialized [8] (i.e., beneficial to themselves rather than to the developer or service [43]). Carrascal speculates that most privacy concerns around digital data arise because of a lack of awareness that personal information is being monetized in certain ways [8]. They go so far as to suggest that the privacy concerns of most users would be tempered if online service providers were explicit and up front about their practices [8]. Prior work supports this idea, showing that the perception of the effectiveness of privacy policies on platforms like Facebook can have an impact on privacy attitudes [52], and that businesses that properly inform consumers about their information handling practices instill greater confidence and reduce perceived risk of privacy violations [54].

However, this kind of transparency is not common practice among online platforms. An analysis of privacy practices and policies for a set of online social networks revealed that privacy is rarely used as a selling point, and that promotion of policies or privacy controls is rare [6]. Moreover, both this study and prior work around privacy policies reveals that they are highly inaccessible due to length, readability, and obfuscating legal jargon [35]. A study of Android permissions confirmed low levels of both attention (few users paying attention to permission) and comprehension (even less being able to answer questions about those permissions) [14]. Bonneau suggests that this is especially problematic because privacy practices vary greatly from site to site [6], an issue that exists not just in privacy policies but in other online terms and conditions [15]. In other words, if a user understands the policies of one platform, they should not assume that similar policies are in place for other platforms.

However, there are often limited incentives for platforms to have more transparent privacy practices, and indeed for them to implement practices that match users' privacy needs. There are clear opposing stakeholders—consumers who want information private, and platforms and advertisers that require profiling of user behavior to drive the market. As a result, privacy solutions often risk breaking necessary business models [30]. For example, monetizing social media data with targeted advertising is the most effective business model for Facebook, despite knowing that it may alienate users; acquisition strategies such as pulling data from WhatsApp illustrates their reliance on capturing user data for revenue [12]. It is therefore not surprising that privacy behaviors have been largely reactive, driven by external pressures such as legislative pressures or bad publicity [11].

In fact, a major theme of prior work is the often negative perception of the intentions of companies that steward data. Even prior to widespread digital data, studies showed that consumers assumed that digital marketers had little concern about their privacy, and had negative perceptions of companies that recorded too much personal data [18]. Consumers had strong negative reactions to companies selling information such as data from supermarket loyalty cards with other companies, indicating a desire to be informed and to have a say about how their data is used [18]. A study of "privacy panic" also showed that one of the major worries includes third parties finding out information [2]. Moreover, even when privacy breaches are the fault of third party developers or even members of a user's social network, they tend to place the responsibility on the platform [52]. One study of "quitting" Facebook found that the major reported reason for doing so was suspicions about the treatment of personal data by the company [47].

In sum, prior work in this space reveals a complex landscape of digital privacy where consumer and user attitudes are influenced by preconceptions, cost-benefit analyses, knowledge of policies and practices, and trust and perception of companies and platforms. The current study considers concrete, immediate reactions to specific data privacy controversies in order to see how these attitudes play out in real-world scenarios.

METHODS

To examine public reaction as part of this study, we collected and analyzed public comments to news articles about two different data sharing and privacy controversies.

News Comments as a Data Source

The publication of news articles online has introduced novel participatory features to traditional broadcast media formats. Comments sections on news websites allow readers to express opinions and engage in public dialogue with journalists and other readers [32,55]. Comments sections are also valuable spaces to study public discussion on a variety of topics (e.g., climate change [27], vaccination policies [38], and public reception of HCI research [49]).

Online news comments provide a way to study public opinion and discourse that is particularly efficient with respect to time and resources compared to qualitative methods such as surveys and interviews [21], making them well suited to the immediacy of public controversies. Moreover, any comment on a news article is a participant-driven response, which research has indicated may be more honest and accurate, and also reveals the issues that matter to commenters [9,21]. The comment section is also a naturalistic setting, which provides ecological validity and is well-suited to studying associations [22]. In examining news comments on articles about HCI research, Vines et al. noted that even misinterpretation of research or technology can be useful, because it "provides a gauge for the political and emotional context of the work beyond the often-homogenous, self-selected and motivated individuals that may participate in the research" [49].

This method also requires the collection and analysis of public data. Though the analysis of public content without consent is common practice within the social computing research community, there are inconsistent norms around issues such as whether it is acceptable to quote content verbatim and even what constitutes *public* data [50]. Although comments on news articles constitute publicly available information, there may be concerns about contextual privacy violation, in that commenters on news articles likely do not consider their comments as participation in academic research [16]. However, in considering this issue we felt that the comments in our dataset are more overtly public than personal social media streams, because they are explicitly addressed to an unknown audience rather than a pre-established social network. Many thematic analyses of user comments include full-text quotes in the published research [9,16,17,49] and we have chosen to include quotes for purposes of best illustrating our themes. Though there is a danger of commenters being identified through quotes with some investigation, we felt that risk is low given that we are not examining inherently sensitive subject matter, and we kept this in mind when choosing illustrative quotations.

Limitations

While there are clear benefits to using reader comment data, there are also potential limitations. For example, there is uncertainty around commenter demographics, particularly for anonymous or pseudonymous comment systems [21], though the need for this information is dependent upon research goals. Another concern is that the tone, content, or frame of the article may influence the comments, though some preliminary research suggests this may not be a significant confounding factor [16,17,22]. There are further known limitations to the quality of discourse found in comments related to issues of access, civility, anonymity, fragmentation, selective exposure, and homogenization [55]. Therefore, though this data lacks the problem of research self selection bias, there are other forms of self selection that could affect the generalizability of the data.

We frame the current study, however, as specifically examining reactions to media portrayals of these controversies. We are interested in how our findings track to previous studies of user attitudes, but do not make claims about generalizability, and our findings should be interpreted with this in mind.

Data Collection

Our dataset consists of public comments posted to news articles on both news organizations' websites and official Facebook pages. We identified a set of articles for both controversies using LexisNexis and Google News, by searching for related keywords and visiting the articles where they were originally posted. Criteria for inclusion were (1) the article was primarily about that controversy; (2) the article was from a news site rather than, e.g., a personal blog; and (3) the article contained at least one comment. For articles on sites that did not have comment sections, we checked for a posting on the organization's official Facebook page and pulled public comments from there instead if available. We also pulled comments from Facebook if available for articles that also had comments posted on their website. If there was more than one public Facebook post from that organization for a single article, we pulled comments from all available posts. In order to not oversample from a single source, if an article had more than 100 comments, we only included the first 100. "Comments" includes both top-level comments and replies. There is a mixture of anonymous, pseudonymous, and non-anonymous comments throughout our dataset. Our final dataset of comments consists of 775 comments (373 WhatsApp, 402 unroll.me), representing 27 unique articles (11 WhatsApp, 16 unroll.me).

We also conducted open coding on the topics and sentiment of the articles themselves. Though topics were constrained to the controversies at hand, we did observe some general categories of content: *advice* (such as explaining how to opt out of data sharing), *reporting on reaction* (focusing on how people have responded to the controversy), and *broader discussion* (using one of the controversies as a catalyst to discuss issues of privacy more generally).

We also considered whether each article was critical of the tech company. We categorized 12 of the 27 articles as "critical" and 14 as "neutral." Only one article (concerning

unroll.me) seemed overtly positive towards the company, expressing surprise that anyone would be bothered by free services selling data; this article represented only 4 comments in our dataset. Overall, comments accompanying "critical" articles made up more of our dataset—477 comments compared to 294 neutral comments. Though prior studies of news comments have suggested there may not be a significant relationship between the content of the article and the content of comments [16,17,22], it is of course possible that article tone impacted commenter reactions. However, in analyzing the comments we found both negative and positive comments across articles of different tones. Even in articles that were overtly critical, some commenters still took the company's side, for example chastising others for not reading policies.

For articles about unroll.me, the average number of comments per article was 15 (median 7), and for WhatsApp 31 (median 15). The average number of *unique commenters* per article across the dataset was 23 (median 14), though we cannot speculate about whether the same commenters might have appeared in multiple articles. The average word count per comment across the dataset is 73 words (median 40, ranging from 2 to 527). We chose the comments quoted in our findings as representative of themes and generally of the types of comments found across our entire dataset. News organizations represented include *The New York Times*, *The Guardian*, *USA Today*, *Lifehacker*, and *Slate*, among others. All articles were written in English, so the data mostly represents the US and UK, with one article from a news organization in India and one from Singapore.

Data Analysis

There are different ways to approach the analysis of comments as established in the literature, though a common approach is a thematic analysis [9,16,22,48,49]. This method reveals patterned responses in data with particular attention to meaning, explanation, and rich description [7]. For this study, we coded themes inductively, working from the data to find commonalities rather than coming in with a particular schema in advance. We largely used individual comments as a unit of analysis, while considering contextual information of threads where appropriate.

Our analysis followed the general recursive steps for thematic analysis outlined in Braun and Clarke, from inductive coding to production of themes [7]. This was an iterative process with two analysts, coding independently and then coming together to memo, discuss, adjudicate differences, and finalize coding schemes and themes.

FINDINGS

Distinct patterns of privacy attitudes and reactions to these controversies emerged through our thematic analysis. Here, we focus on two major themes that encompass a great deal of what is represented in these reactions: differing visions of responsibility for privacy, and strategies for mitigating privacy risks. We also find that view of responsibility typically determines ideas for solutions and strategies, as well as the level of privacy concern expressed.

Responsibility for Privacy

Prior work regarding personal data management shows that there may be a dichotomy of attitudes towards privacy and responsibility—whether it is a consumer's own responsibility to protect their data online or the responsibility of the company with which they are transacting [10]. Kang et al. also found that some participants trust institutions or companies to take care of their security, and other participants suggested that users were putting *too* much trust in the system and should take more personal responsibility [24]. Our findings confirm a contrast in these two visions of responsibility for privacy, and illustrate the specific arguments to support each.

Because the framing of the articles and selection bias of those choosing to comment could have an impact on the relative frequency of different attitudes, we make no claims about which of these might be more dominant in the general population. However, we will note that because the news articles primarily presented the situations as controversies and examples of privacy violations, negative reactions typically either represented (1) negative reaction to the perceived privacy violation; or (2) negative reaction to those having a negative reaction to the perceived privacy violation (either in response to the article or to other comments). The first largely represented visions of company or platform responsibility, and the second visions of user responsibility. The second was somewhat more prominent in our data, so we will discuss it first.

User Responsibility

Many commenters, though agreeing that a privacy violation may have occurred, felt that it was the responsibility of the user to have prevented this violation. This largely boiled down to "you should have known"—because of common sense or because of proper notice from the company.

The phrase "you are the product" occurred over and over again in our data. (In fact, it appeared so frequently that there were multiple comment threads delving into the origin of the phrase.) Commenters typically used this concept as an explanation for how the world works, expressing disbelief that others would not have anticipated that companies would be monetizing their data.

Someone, somewhere has to pay for shit, it's how the world works. [w][1]

Color me shocked that people are too stupid to realize a free service is monetizing the data they collect from you. [u]

Some commenters used this worldview as an explanation for their own behavior, typically expressing that their acceptance of personal responsibility would protect them from privacy violations.

[1] Quotations are presented verbatim and without corrections, with mid-quote shortening represented with […]. Comments from WhatsApp articles are indicated with a [w] and unroll.me indicated with a [u].

That's why I didn't sign up [for unroll.me]. No such thing as a free lunch. [u]

However, though commenters often presented this as common sense, there was also recognition that understanding specific privacy practices requires research.

The responsibility is with the user. If people are to be let loose on the internet they should understand that private companies are there to make money. Before giving a company your inside leg measurement a bit of research is required. As I say that is no one's responsibility, other than the user. [w]

Typically research was conceptualized as gaining familiarity with platform policies. For the unroll.me controversy, there was a provision about data selling in a privacy policy; for WhatsApp, data sharing with Facebook was contingent on agreement to a new policy. A dominant theme among those advocating personal responsibility was scolding users for not reading these policies.

The information certainly was available. It appeared in a terms and conditions pop up that you had to acknowledge and accept. [w]

If it was in the TOS the users only have themselves to blame for not reading it. [u]

Did you read the T&Cs? If not, no sympathy I'm afraid. [w]

It is also possible that some who place responsibility more on the user might have more of an understanding how the technology works. Kang et al. found that people with more articulated technical models perceive more privacy threats—though they may or may not take more action [24]. Though we do not have data to confirm patterns with respect to commenter traits, we will later discuss that commenters with this attitude were more likely to suggest obscure alternative platforms with better privacy features.

Platform Responsibility

The second view of responsibility was that at least some of it should fall to the company or platform. As revealed by our discussion of prior work, consumers often have strong negative reactions to the idea of their data being shared with or sold to third parties without their knowledge. In our data, a major point of difference between those commenters advocating platform responsibility versus user responsibility is what constitutes "knowledge."

Largely in response to commenters pointing out the existence of information in privacy policies and TOS, others pointed to inaccessibility of this information.

You're quite right to say that people are under no obligation to use an app "if they don't like what it's doing". That's fine, as long as "what it's doing" is completely transparent to the user. But often it's not. Plain English isn't a key component of much of the communication on these things. I was recently asked to sign onto a 25-page legal document relating to an app. That's not unusual. [w]

Others pointed out the flaw in a "you are the product and you should know that" argument, that there are some uses of data that are reasonably expected, and others that are not.

That's victim-blaming. You may reasonably expect a free service to, say, show you ads or sell your browsing habits, but it can do anything. ... no one has the time or knowledge to wade through all the TOS and shrinkwraps for every piece of software or music or movie you own, or every account you sign up for. What did you agree to when you signed up for gmail or twitter? Do you know? [u]

Referring to "you should have read the TOS" as "victim blaming" also highlights that commenters with this view of responsibility hold the companies to certain ethical obligations. Some painted the situations as clearly unethical, pointing to "hiding" provisions in legal documents that the companies should know no one reads, or in the case of WhatsApp, purposefully changing the rules once users are already hooked.

Those lengthy, obscure, and legalese Terms of Service have been outlawed in many civilized countries, either by legislative action or by the courts ruling its not reasonable to expect users to be able to read thru these horrors. [u]

[This is] moving the goalposts - app starts in one direction (paid with no adverts) then sells itself to a big advertising company only after you've got all your friends and family joined up, then announced intent to give all the details you submitted under the original premise to its parent advertising company, result is many noses out of joint. [w]

Phelan et al. present one way of considering typical contradictions in privacy concern (e.g., stating an intrusion is "creepy" but also that it does not bother them) as the difference between an initial "gut feeling" versus a deliberate cost-benefit analysis [39]. Factors they suggest are particularly salient for this analysis are trust of the platform, how much they feel "watched" by the platform, and an existing belief that nothing is private online [39]. In our data, the commenters who expect company responsibility often expressed less trust for these companies or did *not* express a belief that privacy is a lost cause.

Strategies and Solutions for Privacy Protection

Within the realm of social media privacy, researchers have considered the strategies that people use to mitigate their own privacy risks, often regarding issues of context collapse or unintended audience [50]. However, our findings here relate not to intentionally shared content but rather to how data might be shared with third parties beyond the original platform.

Faced with these controversies, commenters offered a number of strategies and potential solutions. These differing suggestions also show a dichotomy when it comes to responsibility—what the *user* should do versus what the *platform* or another third party should do.

User-Driven Strategies

Closely tied to placing responsibility on the user, there were three major strategies suggested by commenters for actions for users to take: understanding risks, non-use, and use of alternative platforms.

As previously noted, a number of commenters chastised others for not doing research or reading website policies. A common theme was that if people cared about their privacy, then all they had to do was familiarize themselves with a site's practices and then make an informed decision about whether to use that site. If they choose to use the platform, then they are bound by those policies.

Not really sure why that's a problem…if you don't want to read policies then don't sign up for policies? [u]

Don't really see what the issue is. Private firm asks if you use their service, you play by their rules. Seems fair enough. [w]

The implicit follow-up to this is that if the policies are unacceptable, then they simply should not use the platform. The strategy of non-use to protect privacy was frequent among commenters.

Even better; rest your finger on the Facebook and WhatsApp widgets for a second, then when the little 'x' appears, press that. [w]

Or you can just not use WhatsApp... I refuse to give FB my mobile no. I left Instagram when their privacy policy / ToS debacle happened. Have not missed it. [w]

Use cash. Shop online less. Swipe less. Turn off your 'smart' phone. [u]

Research does suggest that privacy and security concerns are one of the main reasons that people report being offline or quitting social media [4,44]. However, prior work on non-use also tells us why this is not an ideal solution, particularly due to the social cost [4,38]. These counter-arguments were reflected in our data, with a number of commenters replying to non-use suggestions with respect to WhatsApp and Facebook with reasons why they did not want to quit—typically due to reluctance to lose their social connections.

And miss out on a trip to the pub! When someone posts on your local 'Fancy a pint' [Facebook] group. No thanks. [w]

When most of the people you know organise events, get togethers etc through WhatsApp, leaving means becoming an antisocial miserable sod with no friends. [w]

Similarly, with respect to unroll.me some commenters were performing simple cost-benefit analyses. They considered the service to be worth the level of harm they perceived (or did not perceive) of having their data sold.

I love this service and will continue to use it. Anything you use for free is making money off of you in another way. [u]

I really don't care if they sell my anon data. I like the service. My data is pretty boring anyway. [u]

One solution to the non-use counterargument of social cost would be rather than giving up a service altogether to find a similar service. Commenters provided a number of suggestions for alternative platforms, particularly for messenger apps to replace WhatsApp, largely based on criteria of better security and privacy features.

Try Signal. It's developed by the same people who implemented WhatsApp's E2E encryption but don't be put off by that. The guys running the project are all privacy advocates. [w]

I've switched to the Wickr Messenger app. Highly secure, auto deletes messages(and messages sent can be set to auto-delete on the recipient's phone too) and apparent full user security. [w]

However, as we know from Schriener's study on switching from WhatsApp to a more secure messaging system, even with better privacy practices, the cost of switching can still be too high [42]. For this reason, this strategy has limitations.

What about all my friends who have never heard of wickr? [w]

[Wickr is] all great; however, it's hard getting people to switch, despite the WhatsApp data-sharing issues, now everyone's so embedded in it. Users can simply stop using a service but there's a huge resistance to it when all their contacts are on there. [w]

However, despite the counter-arguments to non-use or alternative platforms, non-use appears to be a popular strategy, particularly in *response* to these controversies. There were a large number of commenters who revealed that they stopped using a service.

Thank you! I have linked them to this article in my reason for leaving. [u]

Oh god… switching this off now. [u]

Switched to Telegram once What's App was first taken over by Facebook. It's served me perfectly well since. [w]

So these strategies do seem to be working for some of the commenters in our data set, some expressing relief at having quit or switched away from certain platforms. However, they are also met with the pushback by others noted above. Based on our data, we can speculate that these strategies are particularly unwelcome by those who see privacy violations as the responsibility of the platform rather than the user.

Platform-Based Strategies

Tracking to expressions of platform responsibility for privacy were suggestions that would involve changing their practices or policies. Most often, these suggested changes would be externally imposed rather than self-driven. For example, a number of commenters spoke of what should or should not be "permitted," pointing to the potential for external regulation such as laws.

Sacrificing one's privacy should only be permitted in extreme cases, even if then. It should definitely not be a default condition of using a service, private or otherwise! [w]

App developers should not only live up to a code of ethics, but also to laws that would prevent the tracking and data mining going on. [u]

Our email addresses and contact info are traded and sold to thousands of outfits which harass us day in and day out. This should be illegal - unless we give explicit permission, information about us (including email) should not be for sale. [u]

However, beyond suggesting these externally imposed regulations, some commenters made suggestions around more readable policies or more user-controlled privacy practices.

Instead of celebrating opt-out as if they are doing you a favor… the option needs to be opt-in, with users having to take an affirmative action to opt-in to giving up their privacy. [w]

Typical disagreements with these kinds of suggestions were reminders of business models, pointing out that these uses of data were necessary for the companies to make money: *we are the product*, so if they can't sell us, what is their business model?

Businesses are not charities. So that "free" gmail account, "free" google photos space, "free" unsubscribe service? It's not being run out of the kindness of their hearts. [u]

Others argued that making policies more clear simply would not work, that the problem was not the accessibility of the policies but the apathy of users about privacy.

Put the 'smokers lungs' type warning - it will make no difference. People in the online age are addicted to free (at point of sale) and the overwhelming majority will trade in their privacy to get things free. [u]

This assumption does track to prior work, where after expressing privacy concerns around apps, people were asked why they ignored the end-user license agreements [44]. The answers were that (1) they had never encountered negative consequences from the collection of their data; and/or (2) the desire to have the app trumped their privacy concerns. We saw similar patterns of reasoning in our data.

Reasons for Concern (or Lack of Concern)

Some of the commenters in our dataset were observably upset about the situations being described, and others were not. Those who did not seem bothered largely also fell into the "user responsibility" category, but there were also two major schools of thought: (1) I already knew this was how these things work; and (2) The benefit of the service outweighs the potential privacy cost. Additionally, we propose that most of those who *are* bothered fall into the "platform responsibility" group but also experienced some kind of expectation violation.

These schools of thought are a somewhat remixed version of the categories uncovered by a 2013 study of online privacy disclosures that suggested three types of users: the *scared* who worry about privacy but do not think they have options; the *naïve*, who do not understand what happens to their data; and the *meh*, who understand the trade-offs but are not worried [33]. Our categories translate these kinds of attitudes into how someone might react to a privacy violation scandal.

We have already discussed examples from our data. We actually see two types of people who expressed a lack of concern because they already knew how things work. The first are the "savvy" who featured prominently in our description of user responsibility advocates. They purport to do their research and know what the privacy risks are.

I actually read the terms and conditions before I signed up – or didn't sign up, as it happens. [w]

Others simply have a model of the world where they have very little privacy. We see this in prior work as well, the idea that privacy violations are a given, and once shared, information is simply out of the user's control [19]. This is also a model that Phelan et al. uncovered when considering the salient factors in making privacy cost-benefit analyses, an existing attitude that nothing is private online [39].

I'm neither surprised nor outraged. I mean...it's to be expected. [u]

I assume every aspect of information I put online will be sold to somebody willing to pay for it. [u]

Though this attitude may encourage some to take extra steps to protect their privacy, for others it seems to be more a form of learned helplessness, where they have come to believe that the situation is unavoidable and something that they simply have to live with [44]. Regardless, the outcome is the same: they are unsurprised by the privacy violation and do not intend to take action.

We saw another type of "unconcerned" commenter, who performed a cost-benefit analysis and determined that the benefit of the service outweighs a potential privacy cost. We saw examples of this with people who stated that they liked the service enough to continue using it despite potential harm, or simply saw very little harm in the perceived privacy violation.

What is the damage to me with unroll me selling my non existent lyft receipts to uber? [u]

Too many people privacy where it does not exist… also you have to consider the harm. Selling Lyft your sanitized uber bill? Really? How does that harm you? [u]

However, prior work suggests that when users have a limited ability to infer and understand risks, they are not doing a cost-benefit analysis but rather a "cost justification" [33]. Because many of these users did not know about these practices prior to media attention given to the controversy, they are performing post-hoc analyses. Therefore, their

analysis may be swayed in favor of the platform so as to justify their existing use.

Finally, those commenters who did express concern or outrage tended to have two things in common: (1) they felt that the companies had some obligation to safeguard their privacy and/or provide better information, and (2) the revelation of how their data was used surprised them. Prior work has shown that *expectation violations* are an important part of privacy attitudes [31]. Our observations of a controversy in the wild confirms this concept, since those who had a "this is how the world is" mindset were considerably less concerned than those who expressed their surprise that their data might be used this way. This is reflected in the quotations above about "victim-blaming" where there are only some ways that one might "reasonably expect" data to be used, and the accusation of the company "moving goalposts" in order to trick users. Unfortunately, these expectation violations will continue to be common so long as privacy practices vary so widely from platform to platform [6].

Overall, there appear to be emergent (and possibly recurring) patterns of opinion and argumentation in our data, suggesting that outrage over controversies such as these are less contingent on the nature of the perceived privacy violation and more on existing notions of how privacy is or should be handled online.

DISCUSSION & SOLUTIONS

Our findings about public reactions via media portrayals of privacy controversies support prior work around privacy attitudes and also reveal patterns of arguments and connections between different types of attitudes. In the tradition of privacy research, we see evidence of usability problems related to privacy that can upset users and even cause them to stop using the platform.

First, we consider whether our data suggests that there is a problem here to be solved. Our dataset, which already represented those users who were motivated enough to comment on a news article, included many comments that reflected a lack of concern about the stated privacy violation despite the news articles framing the situation as a major controversy. However, for many, this lack of concern may come from a place of "learned helplessness" [44] where they would like more privacy but have such a poor opinion of the companies that they assume it could never happen. Others expressed that they found a solution in non-use, which is not ideal for platforms that do not want to lose users. It is clear from our study that the type of data sharing represented by these two controversies is problematic for many users. Our findings also suggest the benefits and drawbacks of different ways to deal with this problem.

Is the ideal solution dependent on user action, as suggested by many of the commenters in our data set? Going with the idea of user responsibility would require changing people's behaviors and mindsets. We know from prior work that encouraging people to read privacy policies and terms of service in their current forms would be extremely challenging [15,35]. Some commenters suggested that a basic common sense understanding of business models and "you are the product" would lead to appropriate privacy expectations, though it is unclear how they thought this should be accomplished.

In arguing that the inaccessibility of information about privacy practices actually negates a presumption of this kind of personal responsibility, Simon and Shklovski propose potential solutions that include intermediaries designing tools as well as hard law solutions [46]. This was also a suggestion of commenters, that there should be more externally imposed regulations such as laws or ethical guidelines. There is progress in this area, for example with the General Data Protection Regulation, which goes into effect in 2018 and will unify and strengthen data protection for citizens of the European Union. However, even as progress is made, law can be slow to change and it is difficult to standardize precisely what those laws should be when it comes to online privacy [10,11]. This is also something for which both users and platforms have little control—though policymakers as well can learn from the kinds of attitudes and reactions described in this paper.

Another solution would be for platforms to simply change their practices in order to better align with user expectations—for WhatsApp to *not* share data with Facebook and for unroll.me to *not* sell data gathered from emails. This too presents a clear roadblock. As many commenters pointed out, these companies need to make money somehow. If you are not the product, then what is? However, platforms may still want to consider these expectations and attitudes when they make decisions about business models, to the extent that they can. For example, our findings supported the idea from prior work that with respect to "being the product," users react better to their data being used to improve something for the platform itself (e.g., better advertisements) than it being shared with unknown third parties for their benefit. Phelan et al. also point out that when designers rely on users to *tell* them their desired privacy practices, they typically do not get initial, gut reactions but rather post-hoc analyses [39]. Moreover, beyond business models, companies can always improve their own internal business practices. Work such as the current study to examine initial reactions to real-world scenarios could be helpful to companies trying to understand user privacy needs and expectations.

Finally, the solution most well-motivated by both this study and prior would work be to make information about privacy practices both more contextual and more accessible. If users truly did know how and why their data is being used, then their expectations would be appropriately calibrated. However, as Shklovski points out, simply making terms and conditions more robust or more readable is probably not enough [44]. This is in part because, as shown by our data, people come in with vastly different attitudes towards privacy, with concerns rooted in complex socio-technical configurations.

Though more accessible policies could be a start, our findings suggest that the *what* is less important than the *why*. Commenters who expressed an intuitive understanding of the *why* ("you are the product" or similar) expressed less concern about the practice. This supports prior work that suggests that though users might be more willing to share data if they think it is not being collected at all, once they know about the collection, they are more willing to share if they are given information about the use and purpose [43]. Additional research confirms that information about data sharing that does not specify *who* has access does not provide users with enough information to gauge risk [14]. Therefore, the issue is not so much "make your privacy policy more readable" but the fact that the *why* and *who* are typically not part of the information provided.

If this "what how why who" strategy of providing information about privacy practices could be successful, the different categories of attitudes from our findings suggest that there is little downside from the user stakeholder perspective. Providing users with more information should satisfy those who subscribe to a model of user responsibility and think that other users should simply understand more. Those who place responsibility on the platform, particularly those who complain about the inaccessibility of policies, would likely find this to be a step in the right direction. For those users who still will not read whatever information is presented to them, then at least they will be able to see that an effort was made—as opposed to the backlash we saw related to these two controversies that the information was vague, incomplete, and/or hidden in fine print. More transparency might help those with a learned helplessness mindset to gain more trust in the platform. Finally, with more information, users will be able to perform better cost-benefit analyses.

The potential downside for the platform (aside from the resources involved in implementing such changes) is that if they are upfront with practices that could be unpopular, people will decide not to use their platform at all. In this way, there has always been an incentive structure for obfuscation. However, controversies that spark this kind of public outrage are becoming increasingly common, and in the case of these two situations, resulted in a large number of lost users. Moreover, our data suggests that there is in general a very low level of trust for these platforms, and making efforts to change this could be good for business in the long run.

Another challenge with increased transparency is that it still leaves some burden on the user to make informed choices. However, these choices would be easier if platform practices already aligned with user expectations. This study revealed in part that controversy rises when user expectations are broken; a better understanding of these expectations would also make transparency more beneficial on both sides.

Though we are not the first to propose this kind of increased transparency as a salve for user privacy concerns, our findings provide contextual support from specific scenarios to provide a clear line of motivation to this potential solution. Moreover, since for technology companies, a major downside of privacy controversies is negative media attention, the specific understanding of how user reactions play out in the media may be particularly salient to decision making.

CONCLUSION & FUTURE WORK

Our analysis of "in the wild" reactions to perceived data sharing and privacy violations supports concepts from prior work around issues such as responsibility [10,24], cost-benefit analyses [33,39], the role of privacy policies [6,14,44], non-use as a strategy [39,4,38] trust for platforms [18,47], and expectation violations [31].

Because we were examining concrete reactions, our data has strong ecological validity but often lacks information about motivation or user characteristics. There is a strong case for further qualitative work to validate these user attitudes (beyond comparisons to prior work) based on the rich information we have now about specific reactions. There is also potential for future work in conducting studies with commenters on news articles in order to tease out exactly how media portrayals impact their attitudes.

Additionally, in discussing the trade-offs of potential solutions, we put forth increased transparency about the *why* of privacy practices (in conjunction with increased accessibility of that information) as a solution that could work particularly well in the context of perceived privacy violations around data sharing. Additional next steps would be to study users' reactions to this proposal, as well as to find out more about their information needs, and to conduct usability studies around the best display mode for this information. Our findings also point to the importance of understanding user expectations when it comes to privacy; whether most users agree that it's okay to *be the product* or not, shaping expectations with more transparency could help reduce the frequency of these kinds of privacy controversies.

REFERENCES

1. Alessandro Acquisiti and Ralph Gross. 2006. Imagined communities: awareness, information sharing, and privacy on the Facebook. *Proceedings of the International Workshop on Privacy Enhancing Technologies*: 36–58. https://doi.org/10.1007/11957454_3
2. Julio Angulo. 2015. "WTH..!?!" Experiences, reactions, and expectations related to online privacy panic situations. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.
3. Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. ``Little brothers watching you'': raising awareness of data leaks on smartphones. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*. https://doi.org/10.1145/2501604.2501616
4. Eric P.S. Baumer, Phil Adams, Vera D. Khovanskaya, Tony C. Liao, Madeline E. Smith, Victoria Schwanda

Sosik, and Kaiton Williams. 2013. Limiting, leaving, and (re)lapsing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. 3257. https://doi.org/10.1145/2470654.2466446

5. Allan Bell. 1994. Media (mis)communication on the science of climate change. *Public Understanding of Science* 3, 3, 259–275. http://doi.org/10.1088/0963-6625/3/3/002
6. Joseph Bonneau and Sören Preibusch. 2010. The privacy jungle: on the market for data protection in social networks. In *Economics of Information Security and Privacy*, Tyler Moore, David Pym and Christos Ioannidis (eds.). Springer International Publishing, London, UK, 121–167. http://doi.org/10.1007/978-1-4419-6967-5
7. Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2, 77–101. http://doi.org/10.1191/1478088706qp063oa
8. Juan Pablo Carrascal, Christopher Riederer, Vijay Erramilli, Mauro Cherubini, and Rodrigo de Oliveira. 2013. Your browsing behavior for a big mac: Economics of personal information online. *Proceedings of the International Conference on World Wide Web (WWW)*.
9. Jennifer A. Chandler, Jeffrey A Sun, and Eric Racine. 2017. Online public reactions to fMRI communication with patients with disorders of consciousness : Quality of life , end-of-life decision making , and concerns with misdiagnosis. *AJOB Empirical Bioethics* 8, 1, 40–51. http://doi.org/10.1080/23294515.2016.1226199
10. Ramón Compañó and Wainer Lusoli. 2010. The Policy Maker's Anguish: Regulating Personal Data Behavior Between Paradoxes and Dilemmas. In *Economics of Information Security and Privacy*, Tyler Moore, David Pym and Christos Ioannidis (eds.). Springer International Publishing, London, UK, 169–185. http://doi.org/10.1007/978-1-4419-6967-5
11. Mary J. Culnan and Cynthia Clark Williams. 2009. How ethics can enhance organizational privacy: lessongs from the Choicepoint and TJX data breaches. *MIS Quarterly* 33, 4, 673–687.
12. Kim Doyle. 2015. Facebook, WhatsApp and the commodification of affective labour. *Communication Politics & Culture* 48, 1, 51–65.
13. Catherine Dwyer. 2011. Privacy in the age of google and facebook. *IEEE Technology and Society Magazine* 30, 3, 58–63. http://doi.org/10.1109/MTS.2011.942309
14. Ap Felt, Elizabeth Ha, Serge Egelman, and Ariel Haney. 2012. Android permissions: user attention, comprehension, and behavior. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS).* http://doi.org/10.1145/2335356.2335360
15. Casey Fiesler, Cliff Lampe, and Amy S. Bruckman. 2016. Reality and perception of copyright terms of service for online content creation. *Proceedings of the ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW).*
16. Emma L Giles, Matthew Holmes, Elaine McColl, Falko F Sniehotta, and Jean M Adams. 2015. Acceptability of financial incentives for breastfeeding: thematic analysis of readers' comments to UK online news reports. *BMC Pregnancy and Childbirth* 15, 1, 116. http://doi.org/10.1186/s12884-015-0549-5
17. Nicole Marie Glenn, Claudine C. Champion, and John C. Spence. 2012. Qualitative content analysis of online news media coverage of weight loss surgery and related reader comments. *Clinical Obesity* 2, 5–6, 125–131. http://doi.org/10.1111/cob.12000
18. Timothy R. Graeff and Susan Harmon. 2002. Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing* 19, 4, 302–318. http://doi.org/10.1108/07363760210433627
19. Eszter Hargittai and Alice Marwick. 2016. "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication* 10, 3737–3757.
20. Jojo Hedaya. 2017. We Can Do Better. *Unroll.me Blog*. Retrieved April 23, 2017 from http://blog.unroll.me/we-can-do-better/
21. Natalie Henrich and Bev Holmes. 2013. Web news readers' comments: Towards developing a methodology for using on-line comments in social inquiry. *Journal of Media and Communication Studies* 5, 1, 1–4. http://doi.org/10.5897/JMCS11.103
22. Avery Holton, Nayeon Lee, and Renita Coleman. 2014. Commenting on Health : A Framing Analysis of User Comments in Response to Health Articles Online. 825–837. http://doi.org/10.1080/10810730.2013.837554
23. Mike Isaac. 2017. Uber's CEO plays with fire. *The New York Times*. Retrieved from https://www.nytimes.com/2017/04/23/technology/travis-kalanick-pushes-uber-and-himself-to-the-precipice.html
24. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My data just goes everywhere": user mental models of the internet and implications for privacy and security. *The Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 39–52.
25. Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. *The Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, 1573–1582.
26. Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI).* http://doi.org/10.1145/2470654.2466466
27. Joop De Kraker, Sacha Kuijs, Ron Cörvers, and Astrid Offermans. 2014. Internet public opinion on climate

change: a world views analysis of online reader comments. *International Journal of Climate Change Strategies and Management* 6, 1, 19–33. http://doi.org/10.1108/IJCCSM-09-2013-0109

28. Airi Lampinen. 2010. Practices of balancing privacy and publicness in social network services. *The Proceedings of the ACM International Conference on Supporting Group Work (GROUP)*, 343–344.
29. Pedro Giovanni Leon, Blase Ur, Yang Wang, et al. 2013. What matters to users?: factors that affect users' willingness to share information with online advertisers. *Proceedings of the Symposium on Usable Privacy and Security (SOUPS).* http://doi.org/10.1145/2501604.2501611
30. Ilias Leontiadis, Christos Efstratiou, Marco Picone, and Cecilia Mascolo. 2012. Don't kill my ads! Balancing privacy in an ad-supported mobile application market. *The Proceedings of Hotmobile 2012 13th ACM Sigmobile Workshop on Mobile Computing Systems and Applications*, 2:1–2:6. http://doi.org/10.1145/2162081.2162084
31. Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norma Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *Proceedings of the ACM Conference on Pervasive and Ubiquitous Computing (UbiComp)*.
32. Edith Manosevitch and D Walker. 2009. Reader comments to online opinion journalism: a space of public deliberation. *The Proceedings of the Symposium on Online Journalism* 10, 1–30.
33. Helia Marreiros, Richard Gomer, Michael Vlassopoulos, and Mirco Tonin. 2015. Scared or naive? An exploratory study of users' perceptions of online privacy disclosures. *IADIS International Journal of WWW/Internet* 13, 2, 1–16.
34. Maxwell McCombs and Donald L. Shaw. 1972. The Agenda-Setting Function of Mass Media. *Public Opinion Quarterly* 36, 2, 176–187.
35. Aleecia M. Mcdonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4, 543–565.
36. Jessica Miller, Batya Friedman, Gavin Jancke, and Brian Gill. 2007. Value tensions in design: the value sensitive design, development, and appropriation of a corporation's groupware system. *Proceedings of the ACM Conference on Supporting Group Work (GROUP),* 281–290.
37. Helen Nissenbaum. 2004. Privacy as contextual integrity. *Washington Law Review* 79, 101–139.
38. Jennifer A Pereira, Susan Quach, Huy Hao Dao, et al. 2013. Contagious Comments : What Was the Online Buzz About the 2011 Quebec Measles Outbreak ? *PLoS One* 8(5). http://doi.org/10.1371/journal.pone.0064072
39. Chanda Phelan, Ann Arbor, and Paul Resnick. 2016. It's creepy, but it doesn't bother me. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*, 5372–5384. http://doi.org/10.1145/2858036.2858388
40. Joseph Phelps, Glen Nowak, and Elizabeth Ferrell. 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing* 19, 1, 27–41. http://doi.org/10.1509/jppm.19.1.27.16941
41. Lee Rainie, Aaron Smith, and Maeve Duggan. 2013. Coming and Going on Facebook. *Pew Internet Center Research.* Retrieved from http://pewinternet.org/Reports/2013/Coming-and-going-on-facebook.aspx
42. Michel Schreiner and Thomas Hess. 2015. Examining the role of privacy in virtual migration: the case of WhatsApp and Threema. *Proceedings of the 21st Americas Conference on Information Systems*, 1–11.
43. Fuming Shih, Ilaria Liccardi, and Daniel Weitzner. 2015. Privacy tipping points in smartphones privacy preferences. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI),* 807–816. http://doi.org/10.1145/2702123.2702404
44. Irina Shklovski, Scott D Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. *Proceedings of the ACM conference on Human Factors in Computing Systems (CHI),* 2347–2356. http://doi.org/10.1145/2556288.2557421
45. Irina Shklovski, Scott D Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and creepiness in app space: perceptions of privacy and mobile app use. *Proceedings of the ACM conference on Human Factors in Computing Systems (CHI),* 2347–2356. http://doi.org/10.1145/2556288.2557421
46. Judith Simon and Irina Shklovski. 2015. Lessening the Burden of Individualized Responsibility in the Socio-technical World. *Proceedings of ISIS Summit - The Information Society at the Crossroads*, 1–5. Retrieved from https://sciforum.net/conference/isis-summit-vienna-2015/paper/2885/download/pdf
47. Stefan Stieger, Christoph Burger, Manuel Bohn, and Martin Voracek. 2013. Who commits virtual identity suicide? Differences in privacy concerns, Internet addiction, and personality between Facebook users and quitters. *Cyberpsychology, Behavior, and Social Networking* 16, 9, 629–634. http://doi.org/10.1089/cyber.2012.0323
48. Marisa Torres. 2015. What do users have to say about online news comments ? Readers ' accounts and expectations of public debate and online moderation :

a case study. *Journal of Audience and Reception Studies* 12(2), 32–44.

49. John Vines, Anja Thieme, Rob Comber, Mark Blythe, Peter Wright, and Patrick Olivier. 2013. HCI in the Press: Online Public Reactions to Mass Media Portrayals of HCI Research. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI).*
50. Jessica Vitak, Katie Shilton, and Z. Ashktorab. 2016. Beyond the Belmont Principles: ethical challenges, practices, and beliefs in the online data research community. *Proceedings of the ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW).
51. Laura C. Wilson, Alesha D. Ballman, and Theresa J. Buczek. 2015. News Content About Mass Shootings and Attitudes Toward Mental Illness. *Journalism & Mass Communication Quarterly*, 1–15. http://doi.org/10.1177/1077699015610064
52. Pamela Wisniewski, Xu Heng, Heather Lipford, and Emmanuel Bello-Ogunu. 2015. Facebook apps and tagging: the trade-off between personal privacy and engaging with friends. *Journal of the Association for Information Science and Technology* 66, 9, 1883–1896.
53. Pamela Wisniewski, A.K.M. Najmul Islam, Bart P Knijnenburg, and Sameer Patil. 2015. Give social network users the privacy they want. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW)*, 1427–1441. http://doi.org/10.1145/2675133.2675256
54. Heng Xu, Tamara Dinev, Jeff Smith, and Paul Hart. 2011. Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems* 12, 12, 798–824.
55. Rodrigo Zamith and Seth C. Lewis. 2014. From public spaces to public sphere. *Digital Journalism* 2, 4, 558–574. http://doi.org/10.1080/21670811.2014.882066