Social Characteristics

A Proposed Framework for Social Network Privacy Studies and Ethical Risk Analysis.

Charlotte Swavola

Introduction

Privacy, a term rooted in ethics by definition, describes a zone or status free from public view and attention. Privacy is a sanctuary that overlaps with the perception of self so heavily that it can be considered a right, protected by policy and social norms, though it lacks a firm interpretation. Experiments to define privacy in the online domain incorporate a diverse set of characteristics which makes interpretation of study findings between and among privacy experiments difficult. The intent of this paper is to introduce a framework for evaluation and design of privacy studies with a focus on social network sites. A list of characteristics were elicited from non-social network privacy studies and compared to social network studies to identify a manageable, relevant set. These characteristics were identified as the data recipient, risk of context collapse, and disclosure intent. For each characteristic, two to three values were identified and organized into the proposed framework. This paper defines these characteristics and values and their impact on design, as well as potential ethical risks.

Background of Privacy Experimentation

In the digital age, the privacy can be described as the boundary for the free exchange of information pertaining to an individual or group. Determining this boundary in its many contexts is the first step to defining ethical practices and policies for data collection and handling. However, the contexts in which a definition of "reasonable" or "pragmatic" privacy exists depends on a myriad of dimensions including comprehension, potential harm, risk calculation, the mechanism of collection, etc., resulting in stagnation for online privacy policy development. Fortunately, the sustained growth of the internet economy and the current political environment

have brought efforts to formalize privacy from the ruminations of sociology and psychology to the forefront of ethical debate and data science experimentation. While a cohesive interpretation of online privacy norms may be an unattainable goal, even a rudimentary attempt is necessary for effective policy development and implementation.

The complexity of the issue lends itself not only to experimentation, but to data science specifically in order to expand the breadth of analysis across different populations and online functions. However, given the plethora of established online mechanisms for information transfer and with the diversity of information types, the variety of experimental design offers a tangled definition of online privacy. Correlating these studies and their variables requires a web of interdependencies and assumptions. Some have distilled these into frameworks of core characteristics. These frameworks are critical to interpreting findings from multiple domains and contexts, in hopes of developing a cohesive definition of privacy.

Currently, scientists seeking to characterize privacy have methods such as a taxonomy and analytic tools. Solove's taxonomy focuses on the life cycle of information in the general and digital environment, specifying opportunities for harm or damage (2006), while Mulligan, Koopman, and Doty's analytic tool strives to clarify the function of privacy and its value by evaluating design and guiding debate using a set of dimensions (2016). These methods have been incorporated into applications to evaluate privacy risks in social networks already by assuming some dimensions as fixed and specifying some dimensions as variables. For example Liu and Terzi (2010) utilize sensitivity and visibility in an equation to evaluate the privacy score of members in a social network. The sensitivity variable reference the dimensions of harm as well as Solove's processing activities (Mulligan et al., 2016, and Solove, 2006). The visibility

variable incorporates dimensions of scope and dissemination risk, while assuming collection as a constant (Mulligan et al., 2016, and Solove, 2006). Using these variables to calculate a user's privacy score, Liu and Terzi (2010) have proposed a social-media specific privacy tool for future application development, education, and experimentation. This tool claims to be the first calculation of privacy risk for social network users. However, general online privacy has an expansive experimental repertoire, which could be incorporated into social network privacy analysis using the framework below.

Evaluation Framework

I. Audience or Data Recipient

Privacy experimentation hinges on the transfer of information from an owner or data subject to the data holder. The role this data holder plays and its relationship to the subject is critical when evaluating experiments. This characteristic is defined by three values: digital, peer, and community. These values are based on anonymity as perceived by the subject. For design development, these values point to platform dependencies to achieve the necessary subject-recipient relationship.

The first anonymous value, "digital," describes a data holder that is unknown to the data subject, but cannot be easily attributed to an individual as perceived by the subject or user. This intuitively can represent data warehouses, agencies, or "the cloud" colloquially. Effectiveness for experiments utilizing this data recipient requires specification of how the subject's data will be used by the intended recipient. User comprehension of data holder security, sale of user information, and potential secondary uses falls into its own category of privacy debate, which

includes the effectiveness of "Terms and Agreements" documentation. Even with complete user comprehension, the discrepancy between privacy principles and online behaviors and transactions, coined the privacy paradox by Norberg, Horne, and Horne, has merited its own branch of inquiries (2007). This discrepancy between comprehension and behavior, compounded by asymmetric information of data collection and use (Acquisti, Taylor, & Wagman, 2016), and the precedent of increased dissemination corresponding to increase in quality of services or products (Calo & Rosenblat, 2017), has ample experimental opportunities and ongoing analyses. Analysis using this "digital" data recipient can occur in experiments in which a participant interacts with a website or bot, and their information is transferred into the "unknown." This transaction can occur either directly with an entity, like answering questions to a shopping bot (Spiekermann, Berendt, & Grossklags, 2005) or it can loom as a security risk for shopping sites (Tsai, Egelman, Cranor, & Acquisti , 2010). While these experiments analyze individual comprehension of the data marketplace, existing in it cognitively as bits of data, the privacy calculus changes when they perceive the data holder or potential audience as an individual.

If the data recipient is an anonymous individual, named a "peer" in this framework, the analysis offers insight to the data subject's perception or value of the information transferred. The incorporation of an individual recipient threatens the perceived anonymity of the data subject, as demonstrated by Huberman, Adar, and Fine (2005). The "desirability" of information in this study relates to the "sensitivity" variable used by Liu and Terzi (2010), however the presence of an individual and the risk of judgment changes the value of the information to the individual. In contrast to the "digital" model, which offers a faulty assumption of anonymization or de-identification, the anonymous individual impacts the experiment by shifting the value of

the information transferred. The data subject feels no social pressure to disseminate information or shift their privacy boundary, making this an effective tool to observe what kind of information qualifies as "sensitive," and how that sensitivity varies based on context or application. For example, the physical attributes that were highly valued by some individuals in "Valuating Privacy" may be freely volunteered to an online fitness trainer, where economic information may be more "sensitive" (Huberman et al., 2005). Experiments using this data recipient can effectively correlate to users on social media, as the projected image of self is designed for human interpretation and evaluation, rather than the less intuitive underpinnings of an algorithm.

The final value for data recipient is "community," in which the data subject and data recipient are mutually identifiable peers. This incorporates the human judgment from the "peer" value, but also introduces community pressures, rewards, and risks, as evaluated in the specific social context of the data subject. This social context is critical to the value of the information transferred, as well as the willingness to assume risks in that transaction (Nissenbaum, 2004). In the social context, the endogenous motivations for privacy behavior are functions of intricate social forces, such as imitation or reciprocity (Acquisti, Brandimarte, & Loewenstein, 2015). These specific transactions on social media are not only potentially risky, but abundant as well. Social networking sites accounted for 31% of global internet traffic in 2014- Facebook accounting for 25% of total internet traffic (Pensa & Di Blasi, 2017). Studies utilizing a "community" dynamic can be conducted as an analysis of behavioral data using mathematical models for privacy like that proposed by Liu and Terzi (2010), or by introducing new content as apps or tools that offer behavioral nudges or formulaic privacy guidance, for example (Wang et al., 2013 and Pensa & Di Blasi, 2017).

However, not all social media sites are equally effective as platforms for this experimentation- the size and familiarity of Facebook sets it apart for privacy studies using the "community" data recipient, especially those focusing on dissemination risk across social boundaries. The imbalance of social network site usage is amplified by the function of a community platform. The Facebook network includes twice the number of US users as the next social media site (Figure 1- Pew, 2018). Simply by the size of its network, Facebook eliminates choice of services, a normally critical characteristic of privacy experimentation. Straying from the internet giant would do more than cut down on "likes;" it would instantly fraction the potential social capital of an individual, limiting access to non-redundant information, employment options, and even negatively affecting their mental well-being (Ellison, Steinfield, & Lampe, 2007).

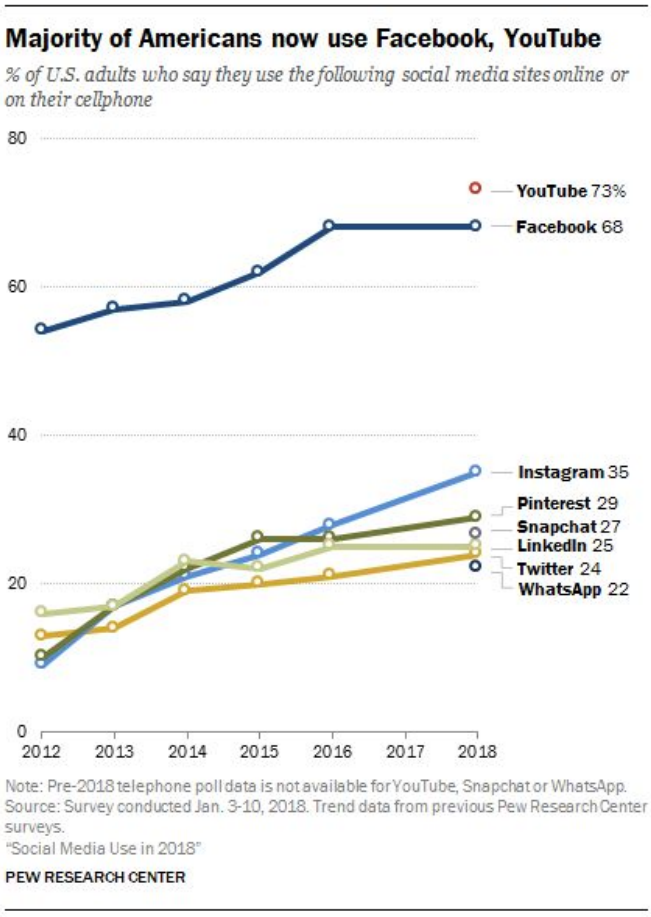

Figure 1- SNS usage chart from the 2018 Social Media Use (Pew, 2018)

The mechanisms of information transfer across the platform vary, and the proportion of use for each mechanism depends on population. According to the 2017 Report on Adults' media use published by Ofcom,

> *"Compared to the average, adults aged 16-24 with a social media profile/ account are more likely to say they like, share or comment on things other people have shared (85% vs. 76%) or to say they create groups or plan events (34% vs. 24%). Those aged 25-34 are more likely to say they post their own comments, share their own videos or photos (86% vs. 78%) or post comments in public groups (32% vs. 24%).*
>
> *Between the ages of 45 and 64, some activities are less likely to be undertaken on social media: posting comments in public groups (15% for 45-54s vs. 24% overall), posting comments or sharing videos or photos (65% for 55-64s vs. 78%) and creating groups or planning events (11% for 55-64s vs. 24%). Compared to the average, over-65s are as likely to say they look at posts without commenting, liking or sharing, or contact organisations to complain, and are less likely to have ever carried out each of the remaining eight activities."* (Ofcom, 2017)

These variations in use may source from different privacy comfort levels pertaining to social boundaries within their demographic, and therefore should be built into experimental design rather than ignored (Mulligan, 2016). While this limits the ability to control avenues of information transfer, it provides an opportunity to observe privacy behaviors of individuals through their preferred interactions. This can be accomplished by designing around a multitude of sharing behaviors and interactions, or by isolating mechanisms and accounting for the potential experimental bias of the participation pool.

Though using Facebook as the privacy testing platform introduces more design intricacies and removes the feature of choice as an experimental mechanism, its magnitude

creates an environment for the privacy risk calculation that most intuitively mimics offline dynamics by engulfing multiple facets, or contextual spheres, of users' lives.

II. Context Collapse

The eruption of social media offers not only a new mechanism of information transfer via data transactions and user interactions, but also through profiles, as the opportunity for self presentation evolves from being based on audience to the potential audience (Goffman, 1959). The multiple identities for various audiences, like coworkers and friends, is packed into one profile, with information accessible across the social media platform. This exposure can be controlled using privacy settings, however awareness and difficulty of use result in content being shared with default privacy settings (Pensa & Di Blasi, 2017). This inherent risk of exposure across the social platform without a clear method to segment the groups can lead to context collapse. The impact of context collapse on user engagement and interaction on social media platforms, namely Facebook, was evaluated by Jessica Vitak as a function of network composition, privacy, and disclosures; a user will evaluate a disclosure and its risk of violating their selected self presentation across their network, against the potential access gain to bridging social capital (2012). The potential bridging social capital and risk of context collapse stem from the blurred boundary of social connections, as well as temporal and spatial boundaries of context (boyd, 2008). This leads to a spectrum of disclosure strategies from disclosing minimal information to avoid violating social norms of any audience (Hogan, 2010), to distributing even specific content to the entire network, ignoring contextual boundaries (Marwick & boyd, 2011). Users, or data subjects, navigate this spectrum on social network sites regularly, urged by

anecdotal (and experimental) evidence of consequences, such as lost employment opportunities, and a desire to maintain the status quo of some communities while engaging or expanding others (Acquisti & Fong, 2015).

A "present" risk of context collapse is the general operating principle of Facebook currently. It grants equal access to members of a network, enabling dissemination of activity or information to intended and potentially unintended audiences. The risk of exposure may be evaluated (or ignored) by a participant based on the algorithm tailored to their attention distribution between their friends, or the information being shared can be evaluated as non-sensitive. An experiment in the form of a Facebook App or Game doesn't have to build in network restrictions, but needs to ensure the "experimenter effect" does not imply an increased level of privacy or security (Spiekermann et al., 2005). Of course, the experimental design must avoid ethical conflicts by requiring users to publicize sensitive content, as the cultural cues of the online community may sway a data subject to violate their own privacy boundary to participate; additionally, content nudged from the subject using site appearance or escalating measures and published to the variable audiences are a potential harm to the participant (Acquisti et al., 2015). Experiments focusing on factors that displace the boundary of privacy should minimize risk in a "controlled" context collapse setting.

The risk of context collapse can be defined as "controlled" if the audience for disclosures is restricted. For example, an experimental design within a closed community, perhaps an approved user list, would have the risk of context collapse controlled. Similarly, if a user engages their privacy settings fully, using features like "Friends lists" on Facebook, which specify permission and access for specific friends, their risk of context collapse could be considered

controlled. In terms of experimental participants, this would have to be true of all participants in the study; still, the exposure risk cannot be eliminated, so the experiment must have policies and frameworks in place to mitigate that risk, such as policies that restrict sharing results of participants, or aggregation of sensitive data before release to other participants. These features can potentially be built into a Facebook App or Game, with strict control over the user lists and viewable data.

Contrastly, the risk of context collapse can be deemed "assumed" or pre-collapsed if the information is automatically shared publicly. This utilizes the contrast concept as a control to evaluate the perceived value of the information being shared (Mulligan et al., 2016). This depends on the user comprehension to avoid ethical risks, including dissemination of information that is co-owned by the user, potentially creating "turbulence" on the accepted privacy boundary, or causing harm by association (Acquisti et al., 2015 and Solove, 2006). Experiments utilizing this value of the "context collapse" characteristic could be particularly effective for determining perceived monetary value of personal information, as the information is not simply given to an anonymous source, but can also be tied to the individual- a level of comprehension often lost by data subjects when transferring information to a "digital" data recipient. However, experiments composed using this value also pose the greatest risk of harm and require the extreme restrictions on content and information transferred.

An important note is the inherent context collapse between the perceived data holder (any of the above values) and the "digital" data holder. While uses cognitively agree to use social networking sites and thus allow the sites to collect and utilize their data and information, data subjects waver between praising and condemning the use of their information to, for example,

improve algorithms that show them relevant content. The context collapse has triggered severe public discomfort when the data amassed by online activity is used or collected in a potentially harmful action, such as aggregating users into categories which may limit their access to non redundant data or exclude them from future activity, or targetting the individual based on profile surveillance for focused content. These harms fit into Solove's framework, however the perceived harm of data collection and analysis through general use implies either lack of comprehension or cognitive dissonance that sharing information with the online community intrinsically disseminates the information to the "digital" platform. This can be compounded by the collection on unintended disclosures by data subjects.

III. Disclosure Intent

The final characteristic relates to the information itself, and the comprehension of the data subject regarding the information. As defined in this framework, this value does not take into account secondary uses or processing of information, as that would require the data subject to evaluate the entire potential of their online presence, rather than the information being volunteered (Correa, Sureka, & Sethi, 2012). Both intended and unintended disclosures have experimental design implications. This characteristic has been isolated from context collapse, though the consequences of a miscalculation are similar in the "community" domain; however, disclosures require separate evaluation of privacy risk. This characteristic is also the most effective for evaluating potential ethical risks and violations in experimental design.

Intended disclosures refer to the voluntary dissemination of information- a property of the information, not the dissemination environment. Intended disclosures may take the form of golf

scores posted on a forum, entering financial information online during checkout, or windows into an individual's social activities or interests. Volunteering this information on social media engages the individual's social network and presents an opportunity to gain bridging social capital (Vitak, 2012). Intended disclosures are not an indicator of truth however, as they may factor into the online "performance" as proposed by Goffman (1959). As noted before, the importance of this performance and inclusion in the community may shift an individual's personal privacy boundaries temporarily, thus intended disclosures of sensitive information must be devoid of community pressures to remain ethical. Intended disclosures also have potentially negative consequences, as interpretation by the target audience is dependent on the members of the audience (Wang et al., 2013). Risks of misinterpretation should be evaluated for potential harm even if the content and dissemination is controlled through an experimental platform or mechanism.

Unintended disclosure refers to unintended information transferred to an intended recipient. This differs from context collapse, which indicates a disclosure to an unintended recipient. Unintended disclosures are caused by a lack of comprehension about the information itself, rather than a miscalculation of risk from dissemination. The information may be owned by multiple parties or implicate others by association- such as a photo of people at an identifiable location, or an emotional post of an individual in a relationship. The intentional sharing of this information may include an unintended disclosure on behalf of the information co-owner, or parties associated to the individual (Acquisti et al., 2015 and Wang et al., 2013). Unintended disclosures can also refer to economic status, or physical location at a specific time. (Wang et al., 2013). Unintended disclosures pose the greatest risk for social network experiment design.

Monitoring content for potential ethical violations before dissemination requires a robust expertise in potential harms as well as technological resources to catch and review potentially harmful content in real time. Still, this risk can be mitigated with a participation policy reinforced by awareness and education, or nudges to teach conservative sharing practices incorporated into experimental design. The risk can also be restricted in a similar manner to "controlled" context collapse by restricting content types or providing a rigid structure for content disclosures.

Conclusion

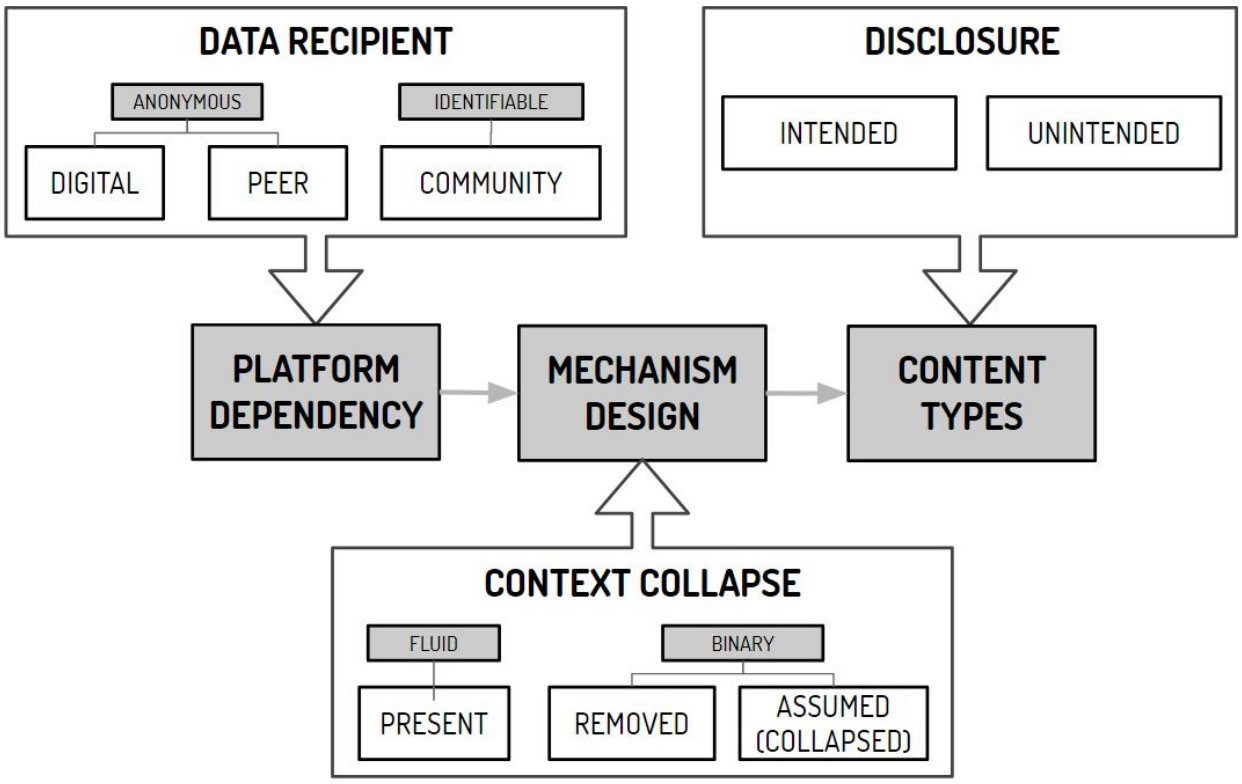

Figure 2- Framework for social network experimental design and ethics evaluation

The new framework identifies relevant characteristics of privacy experiments conducted in a general online domain and organizes them in a social network context. These characteristics are defined by the perception of the data subject as they describe how the subject will interact with the data recipient, evaluate and balance dissemination risk, and their awareness of the information itself. While these characteristics were isolated as a tool for interpretation of non social network studies, the proposed framework and flow (figure 2) can be used as a starting point for experimental design, or to incorporate and adapt existing tools into future studies. Its most critical function is to identify potential ethical violations and privacy risks in experimental design. By evaluating each characteristic as a variable, with the other characteristics' values held as constants, platforms, mechanisms, and content, can be reviewed in order to protect the privacy of data subjects as scientists work to define privacy and ethical data practices.

References

1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). *Privacy and human behavior in the age of information*. Science. Science, 347(6221), 509–514. Retrieved from https://www.cmu.edu/dietrich/sds/docs/loewenstein/PrivacyHumanBeh.pdf
2. Acquisti, A., & Fong, C. M. (2012). *An Experiment in Hiring Discrimination Via Online Social Networks*. SSRN Electronic Journal. http://doi.org/10.2139/ssrn.2031979
3. Boyd, danah M. (2008). *Taken out of context: American teen sociality in networked public*s. Managing, 359(23), 406. http://doi.org/10.1056/NEJMcps0801308
4. Calo, R., & Rosenblat, A. (2017). *The taking economy: Uber, information, and power*. Columbia Law Review, 117(6), 1623–1690. http://doi.org/10.2139/ssrn.2929643
5. Correa, D., Sureka, A., & Sethi, R. (2012). *WhACKY! - What anyone could know about you from Twitter*. In 2012 10th Annual International Conference on Privacy, Security and Trust, PST 2012 (pp. 43–50). IEEE. http://doi.org/10.1109/PST.2012.6297918
6. Cranor, L., Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2007). *The Effect of Online Privacy Information on Purchasing Behavior : An Experimental Study*. Information Systems Research, 22(January), 254–268. http://doi.org/10.1287/isre.1090.0260
7. Ellison, N. B., Steinfield, C., & Lampe, C. (2007). *The benefits of facebook "friends:" Social capital and college students' use of online social network sites*. Journal of Computer-Mediated Communication, 12(4), 1143–1168. http://doi.org/10.1111/j.1083-6101.2007.00367.x
8. Goffman, I. (1959). *Presentation of self in everyday life*, 1–10. Retrieved from http://www.clockwatching.net/~jimmy/eng101/articles/goffman_intro.pdf
9. Hogan, B. (2010). *The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online*. Bulletin of Science, Technology & Society, 30(6), 377–386. http://doi.org/10.1177/0270467610385893
10. Huberman, B. A., Adar, E., Fine, L. R., Labs, H. P., Road, P. M., & Ca, P. A. (n.d.). *Valuating Privacy*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=488324
11. Liu, K. U. N. (2010). *A Framework for Computing the Privacy Scores of Users in Online Social Networks*. ACM Transactions on Knowledge Discovery from Data, 5(1), 1–30. http://doi.org/10.1145/1870096.1870102.
12. Marwick, A. E., & Boyd, D. (2011). *I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience*. New Media and Society, 13(1), 114–133. http://doi.org/10.1177/1461444810365313
13. Mulligan, D. K., Koopman, C., & Doty, N. (2016). *Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy*. Philosophical Transactions of

the Royal Society A: Mathematical, Physical and Engineering Sciences, 374(2083), 20160118. http://doi.org/10.1098/rsta.2016.0118

14. Nissenbaum, H. (2004). *Privacy as contextual integrity*. Wash. L. Rev., 101–139. http://doi.org/10.1109/SP.2006.32
15. Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). *The privacy paradox: Personal information disclosure intentions versus behaviors*. Journal of Consumer Affairs, 41(1), 100–126. http://doi.org/10.1111/j.1745-6606.2006.00070.x
16. OfCom. (2013). *Adults media use and attitudes*. Retrieved from http://media.ofcom.org.uk/news/2013/uk-adults-taking-online-password-security-risks/
17. Pensa, R. G., & Di Blasi, G. (2017). *A privacy self-assessment framework for online social networks*. Expert Systems with Applications, 86, 18–31. http://doi.org/10.1016/j.eswa.2017.05.054
18. Pew Research Center. (2018). *Social media use in 2018*. Retrieved from www.pewresearch.org
19. Solove, D. J. (2006). *A Taxonomy of Privacy*. University of Pennsylvania Law Review, 154(3), 477. http://doi.org/10.2307/40041279
20. Spiekermann, S., Grossklags, J., & Berendt, B. (2001). *E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior.* EC '01 Third ACM Conference on Electronic Commerce. http://doi.org/10.1145/501158.501163
21. Vitak, J. (2012). *The Impact of Context Collapse and Privacy on Social Network Site Disclosures*. Journal of Broadcasting and Electronic Media, 56(4), 451–470. http://doi.org/10.1080/08838151.2012.732140
22. Wang, Y., Leon, P. G., Chen, X., Komanduri, S., & Norcie, G. (2013). *From Facebook Regrets to Facebook Privacy Nudges*. The Ohio State Law Journal, 74, 1307–1335. http://doi.org/10.1525/sp.2007.54.1.23.