Isabell Koinig

“I’m not a kid anymore!”

Towards a teen-centric approach of online privacy management

Abstract

The youth constitutes the largest user base of social media networks. While this generation has grown up in a digitally immersed environment, they are still not immune to the dangers the online space bears. Hence, maintaining their privacy is paramount. The present article presents a theoretical contribution, that is based on a review of relevant articles. It sets out to investigate the importance adolescents attribute to online privacy, which is likely to influence their willingness to disclose data. In line with a “new privacy paradox”, information disclosure is seen as unavoidable, given the centrality of social networks to adolescents’ lives. This goes hand in hand with individual privacy management. As individuals often lack knowledge as to how to protect their privacy, it is essential to educate the youth about their possibilities, equipping them with agency and self-responsibilization. This corresponds with a teen-centric approach to privacy as proposed by the TOSS framework.

Zusammenfassung

Die Jugend bildet die größte Nutzerbasis von Sozialen Medien. Obwohl diese Generation in einem digitalisierten Umfeld aufgewachsen ist, ist sie dennoch nicht immun gegen die damit einhergehenden Gefahren. So ist etwa die Wahrung der Privatsphäre von größter Bedeutung. Ziel des vorliegenden theoretischen Beitrags ist es, zu untersuchen, welche Bedeutung Jugendliche dem Datenschutz beimessen, die offenkundig ihre Bereitschaft zur Preisgabe persönlicher Daten beeinflusst. Im Zusammenhang mit einem „neuen Privatsphäre-Paradoxon“ wird die Offenlegung derartiger Daten angesichts der zentralen Bedeutung sozialer Netzwerke für das Leben von Jugendlichen als unvermeidlich angesehen. Dies geht Hand in Hand mit einem individuellen Datenschutzmanagement. Da Einzelpersonen häufig nicht wissen, wie sie ihre Privatsphäre schützen können, ist es entscheidend, Jugendliche über ihre Möglichkeiten aufzuklären und sie mit Entscheidungsfreiheit und Selbstverantwortung auszustatten. Dies entspricht einem jugendorientierten Ansatz des Datenschutzes, wie er etwa vom TOSS-Framework vorgeschlagen wird.

Keywords: Privacy, privacy management, privacy paradox, agency, teen-centric aproach

1 Introduction

Having grown up in a technologically immersed environment, the youth – as "digital natives" (Prensky, 2001) respectively the "generation always on" (elbdudler, 2018) – has received heightened attention in academia. Conditioned by their avid social media usage and Internet activities (Blank et al., 2014), their online (communication) behaviors have been subject to much scrutiny (e.g., Petronio & Durham, 2008; Robinson, 2016). The Internet has literally led to the emergence of an "electronic panopticon" (Haggerty, 2006), granting the youth not only public exposure but also increasing their struggles as to maintaining their privacy. Youth surveys in Germany (cf. Statista, 2018a) revealed that teenagers aged 14-19 considered data protection either as very important (27%) or important (39%). Similar numbers are reported by the Bravo YouGov study (2018). Albeit privacy and privacy protection seem to be core values for the general population regardless of age, individual behaviors often contradict these claims.

A so-called "privacy pragmatism" has been commonly used to describe both teenagers' and adolescents' behaviors with regard to managing their private information (Raynes-Goldie, 2010). This behavior is characteristic of "people who are concerned about their privacy but are willing to trade some of it for something beneficial" (Raynes-Goldie, 2010). In literature, this phenomenon is discussed as privacy paradox (Barnes, 2006). This suggests that individuals – and especially the youth – have developed a rather lax attitude towards information disclosure, which is usually coupled with a high degree of unawareness as to what could happen with their data (Barnes, 2006).

2 Privacy and data protection

The online world is characterized by a lot of dangers, often referred to as cyber risks (boyd, 2014). These risks are grounded in the affordances of social media, meaning that content is searchable, replicable outside of social networks, as well as accessible to invisible audiences (boyd, 2008; boyd, 2014). Given these dangers and high abuse potentials, individuals have been found to be increasingly concerned about their privacy (Madden & Rainie, 2015; Trepte, 2016). In general, privacy describes "a state of limited access to a person" (Schoeman, 1984) respectively "[personal] data" (Smith et al., 2011) and is regarded as the "selective control of access to the self" (Altman, 1975, p. 18). As such, privacy alludes to the fact that individuals can choose which information about their person is published – and which is not (Nissenbaum, 2009). As "owners" of their information, they have the right to control the access to their data (Petronio, 2002).

A plethora of articles from various academic disciplines have dealt with the topic of privacy in the context of digital communication (for an overview, see Knijnenburg et al., 2013). Previous research (Ponciano et al., 2019) has grouped individuals into different categories, depending on their levels of privacy concern[1]:

1) Privacy concerns refer to individuals' worries as to the negative consequences of sharing information with others (Cho et al., 2010; Zhou & Li, 2014).

fundamentalists (high privacy concerns paired with high distrust in business and technology), *pragmatists* (moderate privacy concerns paired with moderate distrust in business and technology), and *unconcerned* (low to no concerns paired with low to no distrust in business and technology). The youth has been found to widely vary with regard to their privacy concerns as well (e.g., see Walrave et al., 2016).

2.1 Different forms of privacy

In the online context, different forms of privacy regulation can be identified, which grant varying degrees of responsibility to individuals: *privacy by design*, *privacy by default* as well as *privacy as forsaken*. *Privacy by design* postulates that privacy – as a value – has to be taken into account in the development and design process already, while *privacy by default* alludes to the fact that a commercial party is only granted access to data that can be used for specific (limited) purposes (EDPS, 2019). *Privacy as forsaken* portends that – in the digital age – individuals lose control over their data as soon as they post it online (James, 2014). The last aspect has been found to be expressive of the current youth's mindset, for whom two additional categories have been identified: *privacy as social* and *privacy "in your own hands"* (James, 2014). According to the prior category, adolescents announce not to post anything that is of concern, while trusting others not to use the personal information they shared against them. The latter – privacy "in your own hands" – presupposes individualized responses to privacy (James, 2014).

While protecting personal information is absolutely vital for all age groups, it is of particular importance for teenagers and adolescents (Robinson, 2016). Previous research has indicated that when it comes to privacy managements, adolescents' and adults' behaviors are significantly distinct from one another, as the latter engage in more elaborate and sophisticated thought processes as to which data to share (Petronio, 2002). Adolescents, on the other hand, seem to be burdened by the realization that privacy requires some active doing on their part.

2.2 Privacy and the youth

Adolescents are renowned to be active digital citizens, who are "much more active and social with their use of media" when compared to other user generations (Cassidy et al., 2013, p. 594). Studies have confirmed that they share a plethora of information on their profiles, ranging from their name, contact information, over location, to political views and employment information (Peterson, 2010; Steijn, 2016; Robinson, 2016). Teenagers have been found to use social media first and foremost for purposes of self-disclosure. Self-disclosure alludes to an act of providing personal information to other people (Petronio & Durham, 2008; Robinson, 2016) and is central to relationship building (Sprecher & Hendrick, 2004). In the social media context, it describes "the amount of information shared on [a] user's profile as well as in the process of the communication with others" (Krasnova & Veltri, 2010, p. 2). As such, self-disclosure en-

tails a conscious choice to achieve a balance as to which information is disclosed and which information is disguised or concealed (Petronio & Durham, 2008).

"Teenagers will freely give up personal information to join social networks on the Internet" (Barnes, 2006). While this tendency is pronounced amongst individuals of all ages, it is quite characteristic of the younger generation, who – albeit being expressively concerned with maintaining their privacy – has a habit of "oversharing", i.e. disclosing a lot of sensitive, personal information and not utilizing any privacy management practices (Adorjan & Ricciardelli, 2019). This might be conditioned by adolescents' "nothing to hide" attitude, making them not consider privacy as a sensitive and important value (Barnes, 2006; Adorjan & Ricciardelli, 2019). Some authors have even gone as far as claiming that the youth have become less shameless and, thus, do not worry about their privacy at all (boyd, 2014; Livingstone, 2003; Nussbaum, 2007).

Privacy is closely linked to individuals' social lives respectively social norms (Nissenbaum, 2011). Already in 2010, Marc Zuckerberg proclaimed that privacy no longer qualifies as a "social norm" (Johnson & Vegas, 2010), stating that "people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm [i.e. open data sharing] is just something that has evolved over time". Whether this claim holds true, will be scrutinized in the next paragraph.

3 Privacy: control or paradoxical behavior?

Following Trepte (2016), two forms of online privacy attitudes can be identified: (1) *privacy as lost in concerns and* (2) *privacy as a question of benefits and gratifications*. *Privacy as lost in concerns* postulates that individuals are highly concerned about their privacy and aim to protect it by all means (Trepte, 2016). This is reflected in recent statistics, according to which 43% of German adults respectively 47% of German adolescents regard the protection of sensitive, private information as highly important or important (Statista, 2019d). For this reason, they also indicate to share data only selectively (Statista, 2019e). On the other hand, disclosure of private data is also linked to benefits and gratifications individuals wish to obtain in doing so (Trepte, 2016). Research has demonstrated that these benefits predominantly concern self-presentation, social support, attention, friendships and relationships amongst others (Taddicken & Jers, 2011; Ellison et al., 2011; Steinfield et al., 2008; Krämer & Haferkamp, 2011).

Previous studies have shown that user behavior is quite hard to predict. While some studies found no relationship between age and privacy concerns (Phelps et al., 2000; Youn, 2005; Taddicken, 2014; Hoofnagle et al., 2010), other scholars report that younger people are "more likely to know and use privacy protection strategies than older consumers" (Youn, 2005, p. 94). Another set of studies, however, revealed younger people to be "naïve to the effectiveness of [privacy management] strategies" (James, 2014: p. 36).

3.1 Privacy management

In recent years, social networking sites have started to delegate responsibility for privacy settings to users (Baruh & Popescu, 2015), appealing to their individual agency to protect information from their peers (*"privacy in your own hands"*; James, 2014). For individuals, privacy management entails setting up boundaries between what data is accessible and what data is kept private (Taddicken, 2014; Trepte et al., 2015). In the online context, it most frequently refers to the privacy protection measures individuals engage in (Dienlin & Trepte, 2015; Zhou & Li, 2014); Paine and colleagues (2007, p. 532) call these strategies "privacy actions".

A number of studies has shown that privacy concerns drive individuals to implement privacy management practices (Wu et al., 2012; Utz & Kramer, 2009). In most instances, privacy management comprises privacy protection behaviors, which can take a variety of forms (e.g., see studies by Son & Kim, 2008; Lutz & Strathoff, 2014; Spiekermann et al., 2010), including the creation of one or more fake accounts, deleting undesired content, using pseudonyms, offering incorrect information regarding age or location, as well as utilizing advanced privacy settings (Bailey & Steeves, 2015; boyd, 2014; James, 2014; Raynes-Goldie, 2010; Wang et al., 2011). Additionally, teenagers have started to communicate in code, delete posts or comments, temporarily deactivate their accounts (boyd, 2014), disable location services as well as employ self-censoring techniques (e.g., Bailey & Steeves, 2015; Raynes-Goldie, 2010; Wang et al., 2011; Hoy & Milne, 2010; Patchin & Hinduja, 2010) – actions, that are indicative of their (elaborate) technological skill levels (Blank et al., 2014). Similar strategies have been confirmed by recent opinion polls (Statista, 2020d).

One theory explicitly dealing with individuals' privacy management strategies is the Communication Privacy Management (CPM) theory (Petronio, 2002). This theory postulates that privacy describes the balance between information accessibility and retreat (Taddicken, 2014; Trepte et al., 2015), resulting from individuals' privacy rules – describing all strategies individuals apply to control their informational boundaries (Petronio, 2002). As such, CPM theory "makes private information, as the content of what is disclosed, a primary focal point" (Petronio, 2002, p. 3) and is regarded as a "first step toward building a theory of online privacy management" (Metzger, 2007, p. 21).

According to Petronio's theory, individuals base their choices on six principles, namely three assumption maxims (i.e. how individuals manage information disclosure) and three interaction maxims (i.e. the degree of information revealed to others; Petronio, 2002; Petronio & Durham, 2008). Two assumption maxims are of relevance in this context: the conceptualization of private information, alluding to the fact that individuals can purposely decide to keep a selected set of information private (Petronio & Durham, 2008); and privacy rules, which do not only govern which information individuals provide but also influence the establishment of privacy boundaries (Petronio & Durham, 2008). The importance ascribed to selected maxims will then impact

individuals' willingness to accept compromises regarding their privacy by granting others "co-ownership" of their data (Petronio & Ventis, 2017).

3.2 Privacy paradox

In literature, individuals' controversial behavior in terms of data disclosure has received a significant amount of attention, where it is discussed as "privacy paradox" (Norberg et al., 2007; boyd & Ellison, 2007; Acquisti & Grossklags, 2005; Smith et al., 2011; Schütte, 2019). In detail, this paradox refers to individuals who share personal information even though they expressing concern that their privacy might be invaded or harmed – thus, their actions contradict their beliefs (Gerber et al., 2017; Schütte, 2019). As such, the privacy paradox is expressive of "a disjuncture between what is said about privacy and what is done in practice" (Adorjan & Ricciardelli, 2019).

In academia, the privacy paradox has predominantly been discussed in the context of social media and digital technologies (Acquisti & Gross, 2006; Barnes, 2006; Quinn, 2016; Tufekci, 2008). Scholars have identified three primary causes for the existence of the (digital) privacy paradox: (1) a lack of understanding regarding the risks associated with information disclosure, (2) a lack of skills to protect individual privacy, and (3) the relevance of social media platforms to individuals' self-identities (Hargittai & Marwick, 2016). Especially the last point suggests that "cyber abstinence" is not seen as an alternative by teenage users (Adorjan & Ricciardelli, 2019, p. 10), for "the need to be seen is greater than the fears […] about privacy intrusions" (Tufekci, 2008, p. 34).

Contradicting behaviors on behalf of individuals might be triggered for a reason, as granting third parties access to private data usually comes with a "surplus value" (Dinev & Hart, 2006). This surplus has commonly been referred to as privacy calculus – i.e. the cost of using certain services or tools outweighs potential risks of disclosing private information (Dinev & Hart, 2006; Ellison et al., 2011). A premium can thereby either take monetary form (e.g., virtual rewards, special offers; Piwek et al., 2016), or social form (inclusion, participation; Dinev & Hart, 2006). For teenagers, core benefits are social media-enhanced socialization and communication, learning opportunities, and access to a wide spectrum of information (O'Keefe & Clarke-Pearson, 2011).

3.3 Towards a "new privacy paradox"

Authors have argued that in the Internet context "[t]echnology creates privacy issues that appear to fall outside the bounds of our traditional analysis" (Austin, 2003, p. 164). Blank and colleagues (2014) urge for a redefinition of the privacy paradox and propose a "new privacy paradox". As both teenagers and young adults are avid social media users, who regard social media to be a core aspect of their personal identities (boyd, 2010), they are forced to take compromises with regard to information disclosure into account since social media platforms do not provide adequate privacy protection tools (Blank et al., 2014). This then suggests that adolescents and teens, whose lives predominantly take place online, are literally forced to accept privacy invasions in order

to benefit from using social media. Taddicken (2013, p. 268), for example, determined that "for many users, refusal to participate in the social web is not perceived as a possible alternative". As a consequence, the youth is constantly asked to weigh the potential risks associated with data disclosure when compared to the possible benefits associated with being on social media (e.g., Chang & Heo, 2014; Taddicken, 2014; Debatin et al., 2009). The younger generation even regards this "compromise" as unavoidable, as otherwise they would be deprived of connecting with their online peers (Regan & Stevens, 2010). Hence, "the[ir] need to be seen is greater than the fears [they] have about privacy intrusions" (Tufekei, 2008, p. 34).

4 Educating the youth

The previous discussion illustrates that it seems to hold true that privacy is increasingly "in [teens] own hands" (James, 2014), requiring individuals to engage in privacy-protective behaviors (Baruh & Popescu, 2015). Hence, calls to invest in individual skill development have been repeatedly uttered (Morlock et al., 2018; Iachello & Hong, 2007; Benndorf & Normann, 2017; Trepte et al., 2015). Building up individual competencies is seen as crucial, for those who reportedly possess high Internet usage skills have been found to be more likely to change their privacy settings on a regular basis (boyd & Hargittai, 2010). This is particularly true of the younger generation (Madden & Smith, 2010; Blank et al., 2014).

Continuous changes to social networking sites' privacy settings have led to a lot of confusion, challenging users to keep track as to what happens to their data (boyd & Hargittai, 2010; Stutzman et al., 2013). For this reason, scholars propose a paradigm shift, moving away from monitoring and controlling teens (*"privacy as prevention"*; Wisniewski et al., 2017a, 2017b) towards empowering them (Wisniewski, 2018). Adolescents need to play their part in maintaining their privacy, becoming "agentic beings" (Davis & Jurgenson, 2014, p. 476) through the process of self-responsibilization (Livingstone, 2003; Prensky, 2001). Broadly speaking, self-responsibilization alludes to the ways the youth perceives and responds to warnings about potential online harms (Adorjan & Riciardelli, 2019). This participatory approach involves educating adolescents to become "agents of their own safety" (Wisniewski, 2018, p. 2) and is expressive of the fact that "as a society, we often spend so much time worrying about young people that we fail to account for how our paternalism and protectionism hinders teens' ability to become informed, thoughtful, and engaged agents" (boyd, 2014).

Instead of teaching adolescents to practice abstinence to protect them from online-risks, teens should be equipped with skills to make educated yet calculated privacy decisions (boyd, 2014; Wisniewski, 2016). For this reason, researchers have started to increasingly advocate a personalized approach to privacy (Kobsa, 2001; Wang & Kobsa, 2007).

5 Towards a teen-centric approach to privacy

One framework that takes teens' autonomy into account is the Teen Online Safety Strategies framework (TOSS), which aims to resolve the tensions stemming from parental control of teenage surfing behavior by moving towards teenage self-regulation. It intends to create awareness for adolescents' motivations respectively actions to disclose personal information by encouraging self-monitoring (Wisniewski, 2018). *Self-monitoring* is thereby perceived as a resilience strategy, meaning that in spite of perceived risk, individuals are able to thrive (Stevenson & Zimmerman, 2005). Teens also exercise *impulse control*, e.g. by not giving in to their current desires, as they are able to anticipate the long-term effects of their behavior. For this reason, they decide to opt out and not to utilize particular platforms because they associate negative consequences with their use. Finally, *risk coping* suggests that in case of a negative event, the situation will be assessed and appropriate strategies to overcome potential harm will be employed (for a more elaborate discussion, see Figure 1 and Wisniewski, 2018).

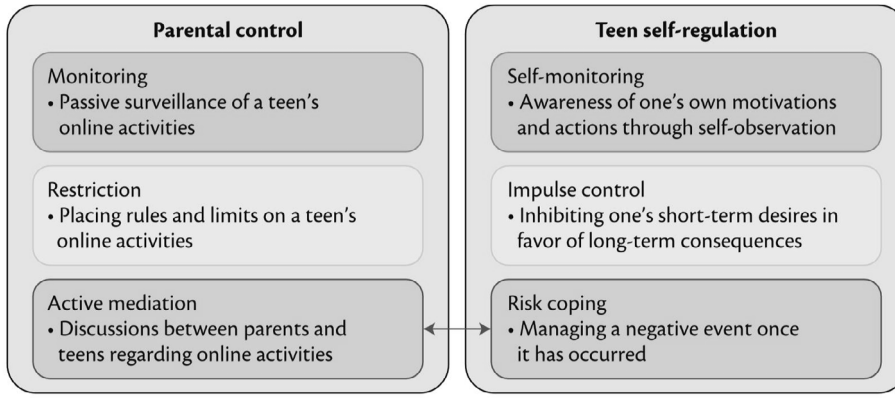

Figure 1: TOSS Framwork (Wisniewski, 2018, p. 3)

While the model suggests moving away from parental control, parents nonetheless can or should play a central role in addressing teens' privacy concerns (Steeves, 2014). A 2016 Pew study determined that "94% of parents say they ever talk with their teen about what they should share online, while 92% say they have ever talked with their teen about what constitutes appropriate online behavior towards others" (Anderson, 2016, p. 4). In order to protect their loved ones, a market for parental control software has emerged, providing parents with the tools to keep their children safe (Hackread, 2016). However, instead of monitoring every move of their children, parents are called upon to pass on the reins and foster teenage autonomy.

Besides "participatory parental mediation" (Ko et al., 2015) or the "value sensitive design" of apps and platforms (Friedman et al., 2013), education and raising awareness are paramount (Wisniewski et al., 2017a). As new technology in general and social

media in particular are an essential part of teenage life (Wisniewski et al., 2017b), parents and teens should build a relationship that is based on trust and mutual understanding. Parents are further asked to award their children both freedom and room for experimentation (Erickson et al., 2015), which would correspond with teens' need for autonomy and development (Wisniewski et al., 2017b).

Overall, the benefits of shared decision making (amongst parents, teens, educators and social networking sites) need to be stressed (Marwick & boyd, 2014). While parents are key actors in educating their children about the necessity of protecting their privacy (Steeves, 2014), schools are central to changing adolescents' "misconceptions" as to not having the power to limit access to their information (Parris et al., 2014). At the same time, the affordances of information systems can assist individuals in managing their privacy (Knijnenburg & Kobsa, 2013). This last aspect is in line with claims by Lampinen et al. (2011) and Wisniewski et al. (2012), who demand service providers to step up and ease the burden put on individuals with regard to managing their privacy.

6 Conclusion

The present-day youth has been brought up in a mindset, which postulates that privacy is something that cannot be achieved in the online context (Adorjan & Ricciardelli, 2019). Studies in support of a so-called "privacy pragmatism" have produced evidence of teens' willingness to trade off some of their information in exchange for a received benefit (Raynes-Goldie, 2010). This compromise seems to be an unavoidable consequence of the "new privacy paradox" (Blank et al., 2014), according to which teenagers are more willing to disclose personal data if they receive some benefits in return (Youn, 2005).

Nonetheless, privacy seems to be in stark contrast with social media affordances (Trepte, 2016). Now more than ever, the protection of individuals' privacy requires an active doing on behalf of the individual, for it is up to them to decide whether they want to grant or deny third parties access to their personal information (Nippert-Eng, 2010). This suggests that every "individual has the ability to decide whether or not someone else needs to know or access something and have her or his wishes followed" (Nippert-Eng, 2010, p. 8). Most social media networks operate on a "public by default, private through effort" policy (boyd, 2014, p. 61), suggesting that it takes some pro-active effort on behalf of individuals to limit access to their personal information. Hence, the protection of privacy presupposes individuals to employ privacy management strategies (Davis & Jurgenson, 2014). For this reason, "developing teens' skills is crucial" (Adorjan & Ricciardelli, 2019, p. 26). Only if awareness amongst teenage users is pronounced, they are able and willing to enforce stricter privacy settings, for instance, on social media (Marwick et al., 2010).

It is important that young adults, as digital natives (Livingstone, 2003), are familiarized with the dangers of the Internet (Blank et al., 2014). Instead of imposing rules on them regarding their privacy management (following a paternalistic approach; boyd, 2014), teenagers should be educated and empowered to take precautionary measures themselves and weigh the consequences of their online participation (Wisniewski, 2018). Their decisions are, of course, not to be seen in isolation, but are bound to the regulatory affordances of social media platforms, which are subject to constant change (Hargittai & Marwick, 2016). Only if teenagers and adolescents are aware of the dangers of the Internet, negative consequences can be mitigated in the long run.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Lecture Notes in Computer Science*, 4258, 36–58.

Acquisti, A., & Grossklags, J. (2005). *Losses, gains, and hyperbolic discounting: an experimental approach to information security attitudes and behavior. Proceedings of the 2nd annual workshop on economics and information security*. Maryland, USA.

Adorjan, M., & Ricciardelli, R. (2019). A New Privacy Paradox? Youth Agentic Practices of Privacy Management Despite "Nothing to Hide" Online. *Canadian Review of Sociology*, February 8–29. doi: 10.1111/cars.12227

Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Publishing.

Anderson, M. (2016). *Parents, Teens and Digital Monitoring*. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2016/01/PI_2016-01-07_Parents-Teens-Digital-Monitoring_FINAL.pdf

Austin, L. (2003). Privacy and the question of technology. *Law & Philosophy*, 22, 119–166.

Bailey, J. and Steeves, V. (Eds.). (2015). *eGirls, eCitizens*. Ottawa: University of Ottawa Press.

Barnes, S. B. (2006). A privacy paradox: Social networking in the Unites States. *First Monday*, 11 (9). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312

Baruh, L., & Popescu, M. (2015). Big data analytics and the limits of privacy self-management. *New Media & Society*, 19(4), 579–596. doi: 10.1177/1461444815614001

Benndorf, V., & Normann, H.-T. (2017). The willingness to sell personal data. *The Scandinavian Journal of Economics*, 120(4), 1260–1278.

Blank, G., Bolsover, G., & Dubois, E. (2014). *A new privacy paradox: Young people and privacy on social network sites. American Sociological Association Annual Meeting, San Francisco, CA*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479938

boyd, d., & Ellison, N.B. (2007). Social Networking Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 210–230.

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

boyd, d. (2008). Why Youth Loves Social Network Sites: The Role of Networked Publics in Teenage Social Life. In D. Buckingham (Ed.), *Youth, Identity, and Digital Media* (pp. 119–142). Cambridge, MA: MIT Press.

boyd, d. (2014). *It's complicated. The Social Lives of Networked Teens*. London: Yale University Press.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2010). *Privacy concerns and information disclosure: An illusion of control hypothesis. Paper presented at the Workshop on the Economics of Information Security*

(WEIS). Retrieved from https://www.researchgate.net/publication/43014896_Privacy_Concerns_ and_Information_Disclosure_An_Illusion_of_Control_Hypothesis

Cassidy, W., Faucher, C., & Jackson, M. (2013). Cyberbullying among youth: A comprehensive review of current international research and its implications and application to policy and practice. *School Psychology International*, 34(6), 575–612.

Chang, C.-W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior*, 30, 79–86. doi: 10.1016/j.chb.2013.07.059

Cho, H., Lee, J., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, 26(5), 987–995.

Davis, J., & Jurgenson, N. (2014). Context Collapse: Theorizing Context Collusions and Collisions. *Information, Communication & Society*, 17(4), 476–485.

Debatin, B., Lovejoy, J.P., Horn, A., & Hughes, B.N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15, 83–108.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45, 285–297.

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

elbdudler. (2018). *Jugendstudie 2018*. Retrieved from https://www.jugendstudie.elbdudler.de/

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R., & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 19–32). Berlin: Springer.

Erickson, L.B., Wisniewski, P., Yu, H., Carroll, J.B., Rosson, M.B., & Perkins, D.F. (2015). The boundaries between: Parental involvement in a teen's online world. *Journal of the Association for Information Science and Technology*, 67(6), 1384–1403.

Gerber, P, Volkamer, M., & Gerber, N. (2017). Das Privacy-Paradoxon – Ein Erklärungsversuch und Handlungsempfehlungen. *Dialogmarketing Perspektiven*, 2016/17, 140–167. Retrieved from https://doi.org/10.1007/978-3-658-16835-3_8

Hackread, K. (2016). *Best choice for teen's cyber safety – parental control app*. Retrieved from https://www.hackread.com/teens-cyber-safety-protection-parental-control-app/

Haggerty, K. (2006). Tear down the walls: on demolishing the panopticon. In D. Lyon (Ed.), *Theorizing Surveillance: The Panopticon and Beyond* (pp. 23–45). Mill Street, Uffculme: Willan Publishing.

Hargittai, E., & Marwick, A. (2016). What can I really do? Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication*, 10, 3737–3757.

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). *How different are young adults from older adults when it comes to information privacy attitudes and policies*? Berkeley, CA: University of California, Berkeley.

Hoy, M.G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising,* 10(2), 28–45.

Iachello, G., & Hong, J. (2007). End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction*, 1(1), 1–137.

James, C. (2014). *Disconnected: Youth, New Media and the Ethics Gap*. Cambridge: The MIT Press.

Johnson, B., & Vegas, L. (2010). Privacy no longer a social norm, says Facebook founder. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Knijnenburg, B.P., Kobsa, A., & Jin, H. (2013). Dimensionality of information disclosure behavior. *International Journal of Human–Computer Studies*, 71, 1144–1162.

Ko, M., Choi, S., Yang, S., Lee, J., & Lee, U. (2015). *FamiLync: Facilitating Participatory Parental mediation of Adolescents' Smartphone Use. UbiComp'15, September 07–11, 2015, Osaka, Japan*. Retrieved from https://dl.acm.org/doi/pdf/10.1145/2750858.2804283

Kobsa, A. (2001). Tayloring privacy to users' needs. In M. Bauer, P.J. Gmytrasiewicz, & J. Vassileva (Eds.), *Proceedings of the User Modeling 2001* (pp. 303–313). Berlin: Springer.

Krämer, N. C., & Haferkamp, N. (2011). Online self-presentation: Balancing privacy concerns and impression construction on social networking sites. In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 127–142). Berlin: Springer.

Krasnova, H., & Veltri, N. (2010). *Privacy calculus on social networking sites: Explorative evidence from Germany and USA. Paper presented at the Hawaii international conference on system sciences, Hawaii.* doi: 10.1109/HICSS.2010.307

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393–411.

Livingstone, S. (2003). Children's use of the internet: Reflections on the emerging research agenda. *New Media & Society*, 5(2), 147–166.

Lutz, C., & Strathoff, P. (2014). *Privacy concerns and online behavior – Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425132

Madden, M., & Rainie, L. (2015). *Americans' attitudes about privacy, security and surveillance.* Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2015/05/20/ americans-attitudes-about-privacy-security-and-surveillance/

Marwick, A.E., & boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, 16, 1051–1067.

Marwick, A.E., Murgia-Diaz, D. & Palfrey, J.G. (2010). *Youth, Privacy, and Reputation [Literature Review]*. Retrieved from https://cyber.harvard.edu/publications/2010/Youth_Privacy_Reputation_Lit_Review

Metzger, M. (2007). Communication privacy management in electronic commerce. *Journal of Computer-Mediated Communication*, 12(2), 1–27. doi: 10.1111/j.1083-6101.2007.00328.x

Morlock, T., Matt, C., & Hess, T. (2018). Perspektiven der Privatheitsforschung in den Wirtschaftswissenschaften. In M. Friedewald (Ed.), *Privatheit und selbstbestimmtes Leben in der digitalen Welt* (pp. 179–220). Wiesbaden: Springer.

Nippert-Eng, C. E. (2010). *Island of Privacy.* Chicago: University of Chicago Press.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, 140(4). 32–48.

Norberg, P. A., Horne, D.R., & Horne, D.A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41, 100–126.

Nussbaum, E. (2007). Kids, the Internet, and the End of Privacy: The Greatest Generation Gap Since Rock and Roll. *New York Magazine*. Retrieved from https://nymag.com/news/features/27341/

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of privacy concerns and privacy actions. *International Journal of Human-Computer Studies*, 65, 526–536.

Patchin, J., & Hinduja, S. (2010). Trends in online social networking: Adolescent use of MySpace over time. *New Media & Society*, 12(2), 197–216.

Peterson, C. (2010). *Losing face: An environmental analysis of privacy on Facebook*. Retrieved from http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=cpeterson

Petronio, S., & Durham, W. (2008). Communication privacy management theory. In L. Baxter, & D. Braithewaite (Eds.), *Engaging theories in interpersonal communication: Multiple perspectives* (pp. 309–322). Thousand Oaks: Sage.

Petronio, S., & Ventis, M. K. (2017). Communication Privacy Management Theory and Health and Risk Messaging. *Oxford Research Encyclopedia – Communication*. Retrieved from https://oxfordre.com/communication/view/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-513

Petronio, S. (2002). *Boundaries of privacy*. New York: State University of New York Press.

Phelps, J. E., Nowak, G. J., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy and Marketing*, 19(1), 27–41.

Ponciano, L., Barbosa, P., Brasileiro, F., Brito, A., & Andrade, N. (2019). *Designing for Pragmatists and Fundamentalists: Privacy Concerns and Attitudes on the Internet of Things. XVI Brazilian Symposium on Human Factors in Computing Systems.* doi: 10.1145/3160504.3160545

Prensky, M. (2001). Digital natives, digital immigrants Part 1. *On the Horizon*, 9(5), 1–6. doi: 10.1108/10748120110424816

Quinn, K. (2016). Why we share: A uses and gratifications approach to privacy regulation in social media use. *Journal of Broadcasting & Electronic Media*, 60(1), 61–86. doi: 10.1080/08838151.2015.1127245

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15(1). doi: 10.5210/fm.v15i1.2775

Robinson, S. C. (2016). iDisclose: Applications of Privacy Management Theory to Children, Adolescents and Emerging Adults. In M. Walrave, K. Ponnet, E. Vanderhoven, J. Haers, & B. Segaert (Eds.), *Youth 2.0: Social Media and Adolescence: Connecting, Sharing and Empowering* (pp. 139–157). Cham: Springer.

Schütte, R. (2019). Paradoxien der Nutzung von IT-Systemen. In B. Blättel-Mink, & P. Kenning (Eds.), *Paradoxien des Verbraucherverhaltens* (pp. 59–84). Wiesbaden: Springer.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly*, 35(4), 989–1016.

Son, J.-Y., & Kim, S. S. (2008). Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32, 503–529.

Spiekermann, S., Krasnova, H., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25, 109–125.

Sprecher, S., & Hendrick, S. (2004). Self-disclosure in intimate relationships: Associations with individual and relationship characteristics over time. *Journal of Social and Clinical Psychology*, 23(6), 857–877. doi: 10.1521/jscp.23.6.857.54803

Statista. (2018a). *Wie wichtig ist das Thema Datenschutz für Dich persönlich?* Retrieved from https://de.statista.com/statistik/daten/studie/867394/umfrage/umfrage-zur-bedeutung-von-datenschutz-fuer-jugendliche-in-deutschland/

Statista. (2019c). *Share of internet users who are more concerned about their online privacy compared to a year ago as of February 2019, by region.* Retrieved from https://www.statista.com/statistics/373338/global-opinion-concern-online-privacy/

Statista. (2019d). *Wie wichtig ist dir die Sicherheit deiner Daten im Internet?* Retrieved from https://de.statista.com/statistik/daten/studie/505798/umfrage/schutz-persoenlicher-daten-von-jugendlichen-im-netz/

Statista. (2019e). *Was denkst Du, wenn es um Deine Daten im Internet geht? Inwiefern stimmst Du den folgenden Aussagen zu?* Retrieved from https://de.statista.com/statistik/daten/studie/804622/umfrage/aussagen-zu-datenschutz-und-sicherheit-im-internet-in-deutschland/

Steijn, W.M.P. (2016). The Role of Informational Norms on Social Network Sites. In M. Walrave, K. Ponnet, E. Vanderhoven, J. Haers, & B. Segaert (Eds.), *Youth 2.0: Social Media and Adolescence: Connecting, Sharing and Empowering* (pp. 117–138). Cham: Springer.

Steinfield, C., Ellison, N. B., & Lampe, C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Applied Developmental Psychology*, 29, 434–445.

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy & Confidentiality*, 4(2): Article 2. Retrieved from http://repository.cmu.edu/jpc/vol4/iss2/2/

Taddicken, M., & Jers, C. (2011). The uses of privacy online: Trading a loss of privacy for social web gratifications? In S. Trepte, & L. Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 143–158). Berlin: Springer.

Taddicken, M. (2014). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, 19, 248–273.

Trepte, S. (2016). The Paradoxes of Online Privacy. In M. Walrave, K. Ponnet, E. Vanderhoven, J. Haers, & B. Segaert (Eds.), Youth 2.0: *Social Media and Adolescence: Connecting, Sharing and Empowering* (pp. 103–116). Cham: Springer.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale". In S. Gutwirth, R. Leenes, & P. D. deHert (Eds.), *Reforming European data protection law* (pp.333–365). Heidelberg: Springer.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20–36. doi: 10.1177/0270467607311484

Utz, S., & Kramer, N. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 3(2), article 1.

Walrave, M., Ponnet, K., Vanderhoven, E., Haers, J., & Segaert, B. (2016.). *Youth 2.0: Social Media and Adolescence: Connecting, Sharing and Empowering*. Cham: Springer.

Wang, Y., & Kobsa, A. (2007). A PLA-based privacy enhancing user modeling framework and its evaluation. User-Modeling and User-Adapted Interaction – *The Journal of Personalization Research*, 23. 41–82.

Wang, Y., Norice, G., & Cranor, L. F. (2011). Who is concerned about what? A study of American, Chinese, and Indian users' privacy concerns on social networking sites. In J. McCune, B. Balacheff, A. Perrig, A.-R. Sadeghi, M. A. Sasse, & Y. Beres (Eds.), *Trust and Trustworthy Computing* (pp. 146–153). Heidelberg: Springer.

Wisniewski, P. (2018). The Privacy Paradox of Adolescent Online Safety: A Matter of Risk Prevention or Risk Resilience? *IEEE Computer and Reliability Societies*, 16(2), 86–90.

Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2017a). *Parental Control vs. Teen Self-Regulation: Is There a Middle Ground for Mobile Online Safety? CSCW '17: Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. doi: 10.1145/2998181.2998352

Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2017b). *Parents Just Don't Understand: Why Teens Don't Talk to Parents about Their Online Risk Experiences. CSCW '17: Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 523–540. doi: 10.1145/2998181.2998236

Wu, K. W., Huang, S. Y., Yen, D. C., & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in Human Behavior*, 28, 889–897.

YouGov (2018). *"Datenschutz-Jugendstudie"*. Retrieved from https://campaign.yougov.com/datenschutzjugendstudiebravo.html

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86–110. doi: 10.1207/s15506878jobem4901_6

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior*, 37, 283–289.