DAVID NAZARIAN
COLLEGE OF BUSINESS
AND ECONOMICS
MKT
Department of Marketing

Satisficing the Privacy of Youth

Kristen L. Walker, Ph.D. & Tina Kiesler, Ph.D.[1]
California State University Northridge

Abstract

We examine the conditions under which parents try to educate and protect their child(ren)'s online digital device use and information exchange. We focus on parental digital literacy and their strategies to protect the digital collection of information about their children. Using a mixed-method approach, we surveyed 54 parents/caregivers of middle school youth and conducted in-depth interviews with ten parents about their online behaviors, their device ownership and use, and their monitoring and online privacy-protection behaviors with their child(ren). The findings demonstrate that parents are concerned, confused, and continually striving to keep up with technology. Yet they increasingly rely on devices and technology to help them monitor their children. They surrender to technology, often leaving gaps in the protection of information shared online and through digital behavior by their children under 13 years of age. Parents are challenged with time constraints and are often unable to carefully consider and implement protection strategies for themselves, making it more difficult to protect their children in their online information exchanges. This hinders their ability to make informed choices on behalf of their children because they lack the digital *data* literacy necessary to adequately protect their privacy. If parents are unable to effectively protect their children's privacy, who will?

[1] This research was funded by a grant to the authors from the Digital Trust Foundation. The authors wish to thank Summer Malone, Andres Nieto, and Charissa Clark for data collection, transcription, and coding. **This is a working paper**. **Please do not quote without permission of the authors.**

"One believes things because one has been conditioned to believe them."
~Aldous Huxley, Brave New World

Technology is omnipresent in the United States and parents play a key role in educating children about the advantages and disadvantages of living a technologically-interconnected life. We examine parents' abilities and challenges to monitor and protect the digital privacy of their children. We posit that parents are challenged by lack of digital literacy and lack of time when it comes to digital privacy and privacy controls, thus leaving youth vulnerable to third-parties who are collecting information and building long-term profiles based on information youth share in their digital media use and online activity.

Current Laws Lack Sufficient Protection for Children Online

Even with the increasing device use and online exchanges of information by youth, the general assumption in the United States is that youth under 13 years of age are protected by legislation, such as the Children's Internet Protection Act (CIPA 2000) and the Children's Online Privacy Protection Act (COPPA 1998, amended 2013). Thus, Facebook, Instagram, Twitter, Snapchat, YouTube, video games and other social media use by youth under the age of 13 are supposed to be limited by design. Yet these limits have not prevented American youth from using social media. Quite the contrary, not only do youth use social media, but in many cases children are more tech savvy than their parents or teachers, and even hide information they exchange online from their caregivers. This is amplified by the lack of understanding by individuals of any age about the risks and potential harm of online information exchanges.

Not only are youth online and actively and passively exchanging information under the age of 13, but they are using platforms and applications that are targeting a broad market. For instance, in describing the 2016 United States v InMobi case, Jessica Rich, Director of the Federal Trade Commission's (FTC) Bureau of Consumer Protection explains, "InMobi tracked the locations of hundreds of millions of consumers, including children, without their consent, in many cases totally ignoring consumers' express privacy preferences" (FTC file no. 152-3203). While some may assume sites and apps that explicitly target children will responsibly protect their digital privacy per COPPA, there is evidence of breaches of that trust, allowing third parties access to persistent identifiers of children under the age of 13 (cf United States v LAI Systems, LLC and United States v Retro Dreamer). These companies were valuing their own economic benefit over the privacy of the children. Violations of COPPA such as these leave parents in charge of their children's digital data, yet unprepared for handling the complexities of privacy and technology.

The issues involving social media use by pre-teen youth are significant and increasing in importance with the increasing prevalence of the Internet of Things (IoT). As more devices become part of daily life for users of all ages, the IoT creates considerable issues around prevention and protection for users 13 years of age and younger. The fact that parents are responsible for their own privacy protection *and* that of their children is problematic in an era when time and information are valuable assets and some parents are even looking to connected digital devices to save time and enhance safety and security.

Social media industry efforts to engage youth in online information exchanges are substantial. Across racial and ethnic groups, young people use social media daily to stay connected to friends, family, and their academic community by sharing elements of their lives. New apps are designed daily and are readily available for youth to download. Photos and videos are forms of social currency and their use is increasing. A 2013 Pew Research report indicates 54% of internet users had posted their original videos or photos to sites while 47% posted video or photographic content from other online sources (Duggan 2013). Snapchat and Instagram are examples of social media platforms that are extremely popular with young online users. A 2014 report by Edison Research states that 43 percent of youth 12 to 24 years of age are Snapchat and Instagram users (The Infinite Dial 2014). As use increases, young people share greater detail about themselves with their friends online, often not understanding that they are also sharing that information *with* the social media organizations and others. In November 2014, Snapchat launched “Snapcash” allowing peer-to-peer payments through Snapchat. The addition of actual currency to the social currency of written information, videos and photos is further cause for concern. Whether parents are aware of these innovations in social media and whether that knowledge influences their approval or assistance when their children (under the age of thirteen) wish to be on social media is an important area of academic inquiry.

While research on teens 13 years of age and older is common, research on device ownership, use, and perceptions of online risk among youth in middle school (or younger) is limited (Youn 2008). Further, research on parents and their role influencing and enabling youth privacy is lacking. For example, the most recent national survey on digital youth was by Pew (Lenhart 2015) and dealt with teenagers (ages 12-17). Notably, research with children is challenging due to the restrictions and institutional review board requirements to protect young participants.

Parents are Digital Educators and Protectors

Parents are significant influencers and enablers of youth digital device use and online activities. Parents (mothers, at least) also spend more time online than others and consider the Internet the *most essential* medium compared to television (Edison Research, Moms and Media 2015). The purchase and use of IoT devices by parents are increasing with 57% of parents reporting that these devices *make life easier*, 36% indicating they *save time*, and 23% responding that they are *useful for safety and security* (Baby Center 2017). Among those who own IoT devices 36% of parents agreed that these devices *help improve parenting*. A variety of apps and platforms exist to help parents protect their kids by monitoring online use. (For instance, Wisniewski et al. (2017) discuss 75 such Android mobile apps.) Yet only 23.2% of parents report using software to monitor their kids, only 35.6% monitor kids in person, and 34.4% of parents do not keep track or monitor their children's online use and behavior at all (Intel Security 2017). Interestingly, in addition to serving as a gateway to a child's digital use and online activity, parents/caregivers are also relying on the same technology to increase their personal convenience and enhance the safety and security of the family. This may prove to be an interdependent security issue if the apps designed to help parents protect their children are also collecting persistent identifiers.

The Internet of Things Overwhelms Parents

In a December 2016 survey of expectant parents and parents with kids under the age of five, 71% reported owning at least one device in the constellation of the Internet of Things such as a smart TV, a home security system, virtual assistants, smart kitchen appliances, and so on (Baby Center 2017). Parents today often face a world where they are digital immigrants raising children who are not just digital natives, but also mobile natives (cf., Morrison 2015). Children are now active consumers online, playing games, watching videos, doing homework, talking to their friends - exchanging a lot of information, often at a rapid rate. They face a world of constant connectedness through use of a variety of interconnected devices. As companies try to develop personal relationships with consumers by collecting information directly and indirectly (through data brokers), we explore the influence parents have over their children's exchanges of information online. *Do* parents try to protect the digital privacy of their children online? *How* do parents protect their children online? Do parents even know *from whom or what* to protect their children?

Surrendering to Technology

Parents and caregivers are managing myriad responsibilities, both personal and professional, as well as the activities and responsibilities of their children. As previously mentioned, parents often look to technology to help manage these activities. Yet there are challenges with technology as well. In the public policy domain, Walker (2016) presents a concept we find useful for framing these challenges called *Surrendering to Technology* (see constructs in Table 1). Outlining the challenges with complexity and context in online information exchanges, Walker proposes that individuals lack the time to pay attention to the details in their online information exchanges and as a result are not making decisions that are protecting their online identity. This complexity influences and is influenced by context, which refers to the uncertainty people experience about their online information exchanges (i.e. the details of where and with whom their information is exchanged) and thus they face vulnerability and risk in their online interactions.

Table 1
Constructs Involved in Surrendering to Technology

Surrendering to Technology	
CONTEXT	COMPLEXITY
Vulnerability and Risk	Continuous Partial Attention
Uncertainty	Cognitive Miser

Source: Walker (2016)

We posit that parents are uncertain about their exchanges of information online, they are unaware of what happens to their information, and they lack the time and attention necessary to make informed decisions – they are surrendering to technology. If parents are surrendering to technology with their own online interactions and exchanges of information, we believe this means parents are going to struggle with their ability to protect their children in their online interactions or enhance their children's digital literacy. We believe that parents' own digital literacy challenges will impact their ability to model or influence their kids' digital literacy. If digital literacy is difficult to attain, this increases the risks youth face while connected.

Protecting Youth Requires Digital Data Literacy, Time, and Effort

There are several definitions of digital literacy, but in general it is used in early education to describe the ability to handle a computer, to understand how to use information and communication technologies to "find, evaluate, create and communicate information" (Clark and Visser 2011). Part of digital literacy is measuring the level of competence an individual has with the "knowledge, skills, and attitudes (KSA's) connected to various purposes, domains[2], and levels" (Shopova 2014). Digital literacy becomes even more complicated since the level of competence can vary between and within an individual's purpose, domains, and levels. Ng (2012) proposes The Digital Literacy Model to clarify the intricacies of digital literacy. The Digital Literacy Model includes three concentric areas of digital literacy: cognitive, technical, and social-emotional. What Ng's model does not address is the knowledge of and risks involved with third parties and the collection, storage, and dissemination of personal data. While Ng's Digital Literacy Model broadly addresses "reproduction and branching literacy," it is unclear whether these topics are well understood by parents/caregivers. Therefore we consider digital *data* literacy as a critical element in the ability of a parent to successfully protect persistent identifiers of their children. Without digital data literacy parents lack the knowledge necessary to adequately protect their children's digital privacy.

To frame our study, we examine how well parents understand risks associated with online use as well as their ability to find, access, evaluate resources, create media, and

[2] Domains refer to daily life or work, privacy and security, and legal aspects.

communicate with others online—their digital literacy. In 2016, parents of K-12 youth planned to spend for back-to-school an average of $343 on technology, $173 for telecom (web/internet) and an additional $216 on mobile devices (Rubicon Project, "Back-to-School Consumer Pulse 2016). In essence, they are increasingly reliant on technology for convenience. This reliance may stem from the fact that parents are overloaded with information, they lack time, they have divided attention, and they are often overloaded with the myriad of third-parties, affiliates, and/or databrokers involved in online exchanges of information. For this reason, we also apply the concept of surrendering to technology in our study (Walker 2016).

Respondents & Methodology

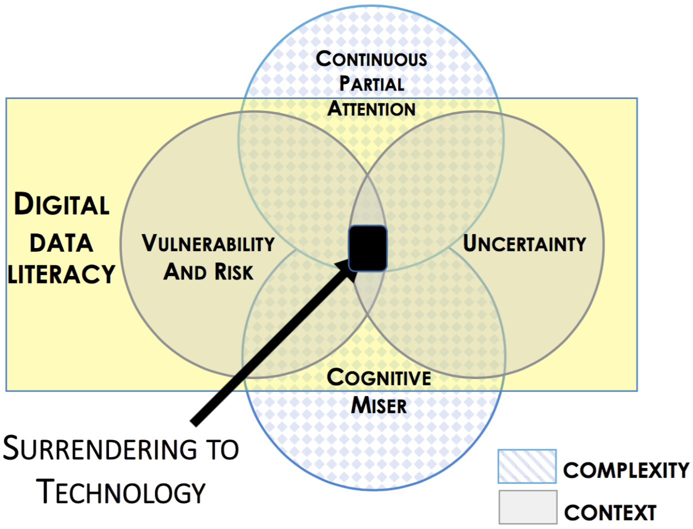
The data reported here were part of a larger study on youth digital privacy funded by the Digital Trust Foundation in 2016. The research project began with six focus groups of 3-5 middle-school age youth from three school districts regarding use of digital media (social media use in particular). Qualitative data from focus groups were analyzed to ascertain patterns and highlight themes and to assist in designing surveys for middle-school youth[3], their teachers and parents/care-givers. In this paper we focus on the results from the parents and caregivers. Parents were from five school districts in a large U.S. west coast city.

We then surveyed 54 parents of middle-school aged youth about their device ownership and use, their online social media habits, and monitoring/protection activities of their children's online activity. The surveys were followed by one-on-one interviews with 10 parents/caregivers of at least one middle-school aged child. Interviews were transcribed (numbered as parents 1-4 and 6-11) and then coded by independent research assistants for analysis (Bogdan and Biklen 1992). Coding schema was developed from digital literacy and

[3] The surveys resulted in responses from 219 youth between the ages of 10 and 13 about their decisions to adopt/use social media, family policies regarding its use (if any), and actual online and interpersonal behavior.

surrendering to technology constructs. These led to two basic themes, context and complexity. Context relates to the knowledge and perceptions parents have of technical literacy (third-parties gathering, storing, and disseminating information) as well as their feelings or knowledge of risks while complexity impacts parents' desire and ability to protect their children during online information exchanges.

Figure 1
Digital Data Literacy & Surrendering to Technology



Findings & Discussion

Results are discussed in terms of context and complexity themes per Walker (2016).

Context

Understanding/Knowledge of Privacy Risks

Parents do not have a clear sense of the privacy risks associated with information exchanges online and this significantly influences their ability to model protection behaviors and to educate middle-school youth about the risks and vulnerabilities of exchanging information online. Parents *do* recognize that there are advantages and disadvantages to their children's use of digital media. Most of the parents interviewed discussed risks such as cyberbullying and what they call "stranger danger." For instance, parent #4 said,

> *You don't know who is behind the handles like on Snapchat, their 'friends' could be a 12-year old or a 60-year old…Some apps are not good and help kids sneak around their parents' backs.*

There was general confusion about digital devices and whether or how they exchange information with others. There was little awareness of passive sharing (via passive listening, monitoring, cookies, and so on). Issues concerning data brokers and third parties collecting and exchanging information from youth online activity and the permanence of a child's online profile were rarely recognized. Few parents mentioned smart appliances (such as TV, nest, refrigerators, and so on) when asked about connected digital devices and appliances in their homes even though ownership of smart appliances came up later in discussion, indicating the connected nature of those appliances may not be top-of-mind for parents. When asked about wearables and smart appliances, parent #3 (with children unsupervised with their own devices at 5 years of age) said, "I don't even know what that is."

Several parents exhibited confusion about the cloud and where information "goes." For instance, parents were asked what they knew about the cloud. parent #4 said, "That's part of the iPhone, right? The backup?" Parent #6 mentioned, "Somehow shutterfly becomes my cloud. I upload a lot of pictures there." Parent #1 confessed confusion and stated,

> *I might be using the cloud. I might not be aware I'm using the cloud. I kind of understand the concept of it but don't quite know all that it accesses.*

When asked how they would delete information, parent #1 said, "Can you even delete [a post on Facebook or Instagram]? I don't know that you can permanently delete it. I wouldn't even know how to do that."

Vulnerability and Risk

Almost all (96.3%) parent survey respondents told us they require their child to share digital passwords with at least one caregiver, indicating they are actively attempting to monitor the child's *gateway* to digital use. Parents tell us they try to limit and monitor their children's online activity, although some say they *track* rather than monitor their children online. In one example from our interviews, the child of parent #8 received his first cell phone because he was walking alone from school to the library and his parents wanted to be able to track him. Somewhat paradoxically, most parents indicated that the biggest advantage of giving their children mobile devices was the ability to communicate and locate their children (which means third-parties may also be able to geolocate the children while they are exchanging information online). Further, most (63%) of the parents surveyed did *not* limit digital use to specific areas of the home, such as public areas that ease monitoring.

Parents voiced concern about the type of information their children would come across while using digital devices. As parent #10 said,

> *Nowadays it is a way [using the internet] to get in touch with minors, and that's my biggest fear. That's why I tell them anytime you see something weird to come and tell me so we can solve the issue.*

It is notable that this parent is planning to address a problem once the problem presents itself to the children and the children decide they have experienced something "weird."

When parents tried to be proactive and monitor their child's digital device use to times when a parent was present, they experienced challenges in controlling their child's behavior. As parent #6 said,

> *It is really like a can of worms. I don't want them to even open them at all but you don't want them to be in the dark neither (sic), they have to know how to navigate and be exposed.*

Another parent (#7) said, "You really can't control them too much, they'll do what they want." Parent #2 said,

> *Last year [her daughter] was locking herself in the bathroom. I originally thought, 'Oh, how sweet. She's becoming aware of her body. She's in there doing body stuff.' And then I realized she was in there doing iPad time secretly. It was funny because you think kids would be embarrassed to be caught masturbating but instead she's embarrassed to be caught using her iPad. These are modern problems right here.*

We asked parents about their specific protection strategies (if any) and discovered a great deal of confusion. As an example, parent #2 has a smart TV with Roku at home as well as, "a couple of laptops, MacBook's, an iPhone, an Android, an iPad, and two desktop computers." When asked about data protection strategies, the parent said,

> *I've been put on the do not call list but I don't know if that counts [as an act that protects data]. One way that I protect my data, totally old school, is by not carrying around those store cards that you'd sign up to get discounts for when you get shopping (sic) by being on their mailing lists. I'm just over it. I don't want them to track me.*

Many parents claimed helplessness, surrendering to the digital environment. In one instance, parent #1 said,

> *I've looked at a lot of stuff like articles and stuff like that. I talked to my husband about what we should do and then we end up doing nothing…It's kind of one of those things where I want to put my head in the sand and not think about it.*

One parent (#10) uses no privacy settings on the browser while another (#4) simply and sadly states, "I know there's no safe place".

Complexity

Ability/Confidence in Role as Privacy Protectors

Parents know they are struggling with their own digital literacy, leaving them with little power to protect the digital privacy of their children. We asked parent survey respondents to tell us how much they agreed or disagreed with several statements (on 5 point scales where 1=strongly disagree and 5=strongly agree). Their mean response to "I know my current privacy settings" was 3.98, indicating they feel knowledgeable about their own privacy control behavior. They agreed (mean=3.70) with the statement, "I don't feel my privacy settings protect me enough." Thus, although they know their privacy settings, they do not feel protected enough by those settings. When asked, "I don't have enough time to update my privacy settings as much as I'd like," respondents were neutral (mean=3.19) with a standard deviation of 1.44. Thus, time management may play a role in some parents' ability to mediate their own risks online and thus it is likely to affect their ability to mediate the risks their children experience online as well.

Our interview data further support the knowledge limits and the time constraints in parents' lives that challenge their abilities to protect the digital privacy of their children. One parent described his/her knowledge limits regarding YouTube, a site children often use for school assignments, "YouTube is like the wild west. I don't know how to monitor that so that's not managed. I close my eyes to what they see on that." Meanwhile, in a different family, an 11-year old daughter has her own YouTube channel (parent #11). Another parent (#2) alluded to time tradeoffs when s/he said,

> *I'm not one to put a lot of research into it [a particular app of interest to the child] but it's okay with her then it's okay with me…I'll let her play and that's because other parents have allowed it with their kids.*

This parent figured that an app was also okay if other parents allowed it with their kids, thus simplifying the decision for this parent. To more easily deal with decisions regarding their data privacy decisions, many parents utilized heuristics—simplifying decisions rules—to determine their course of action. For some families that means the parents are the keeper of a password. As parent #9 said,

> *She [a 12-year old] uses the iPad but she doesn't know the password. I guess that's considered supervised.*

Some looked to the child's school to lead the way. According to parent #1,

> *Their school computers are very battened down. But I haven't checked the privacy settings of those. But I should.*

And some chose to rely upon the reputations of sponsoring organizations, such as the case with parent #2 who told us her daughter is

> *really into Animal Jam. That's the game that all the kids her age are into. It seems safe…it's sort of a social networking game for kids. National Geographic does it and*

> *they are very on top of monitoring it.*

Some left the decisions up to a family member. Parent #9 said, "My wife set something up in there" (regarding privacy settings) and another parent said, "My husband has protections on all of their devices, so they can't supposedly look up bad things." And still other parents leave it up to the kids. Parent #6 shared,

> *I don't have a clear guideline but I would definitely tell [the children] to keep to age appropriate content. I give certain discretion to them and they usually stay within their child programs.*

Parent #8 relies on Google to indicate whether there is any weakness in privacy controls. She told us, "I think [my privacy controls] are adequate. I Googled myself to see how much I can see." Clearly the focus is on recognizable public informational breaches. Third party collection, integration, and dissemination to other parties would rarely show up in a Google search. But it gives this parent comfort to know sensitive information does not come up when she Googles herself (this also demonstrates the use of a brand name as a verb for searching online, exacerbating potential confusion).

Since children often rely on their parents to understand and set up their privacy controls, parents' lack of understanding of privacy controls and lack of time to update their own privacy controls and understand the information sharing policies of their children's digital media, indicate a need for policy to assist in protecting the digital privacy of our youth.

Conclusion

We find that parents have embraced devices and technology to help them monitor their children. Yet, they surrender to technology, often leaving gaps in the protection of information shared online and through digital behavior by their children under 13 years of age. Parents are challenged with time constraints and are often unable to carefully consider and implement protection strategies for themselves, making it more difficult to protect their children in their online information exchanges. As a result, companies and third parties are developing profiles of digital users when those users are young children.

We find that parents lack understanding and knowledge of current digital literacy concepts involving cognitive, technical, and social-emotional constructs. Perhaps more importantly, they lack understanding and knowledge of the multitude of organizations (e.g. databrokers, third-parties, affiliates) that gather, store, and disseminate information gathered from online information exchanges. This puts youth (and parents) at significant risk and allows for long-term vulnerability to unknown harms. The uncertainty about these harms also puts both parents and children at risk. Thus activities that encourage parent and youth education about *digital data literacy* are essential.

Although legislation exists to protect youth under 13 years of age, current online behaviors of children and their parents negate the usefulness of those protections. As a result, we believe further education is necessary of youth and their parents. However, education alone will not solve the issue since parents feel they lack the time to educate themselves about digital privacy and to engage in actions to protect information shared with unknown others by their children through both passive and active online activities. They have surrendered to the technology and as a result, policy changes are necessary to better protect the information shared by young children in online and digital environments.

More regulation is necessary since parents and children are interdependent in their privacy naiveté. As Jessica Rich, Director of the FTC's Bureau of Consumer Protection points out, "It is vital that companies understand the rules of the road when it comes to handling children's personal information online." While the FTC is concerned about the rules of the road, parents don't know where the road is or where to turn. With the Internet of Things, parents will need a more detailed road map.

References

BabyCenter Global Parents' Panel, The BabyCenter Community, and the Research Now panel (December 2016). "The Internet of Things Empowers Parents" Available at: https://www.babycenter.com/0_71-of-todays-parents-own-at-least-one-internet-of-things-dev_10

Bogdan, R., & Biklen, S. K. (1992). *Qualitative research for education: An introduction to theory and methods*. Boston: Allyn and Bacon.

Children's internet protection act (2000). Information available at https://www.fcc.gov/guides/childrens-internet-protection-act.

Children's online privacy protection act (1998). Available at: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.

Clark, L., & Visser, M. (2011). Digital literacy takes center stage. *Library Technology Reports*, *47*(6), 38-42.

Duggan, M. (2013, Oct 28). Photo and video sharing grow online. Pew Research Center report. Available at http://pewinternet.org/Reports/2013/Photos-and-videos.aspx

Edison Research "Moms and Media 2015" (January 2015). http://www.edisonresearch.com/wp-content/uploads/2015/05/Moms-and-Media-2015-Final.pdf

Huxley, A. (1998). Brave new world. 1932. *London: Vintage*.

Intel Security (January 24, 2017). "New Family Dynamics in a Connected World." https://www.mcafee.com/us/about/news/2017/q1/20170124-01.aspx

Lenhart, A. (2015). Teens, social media, and technology overview 2015: Smartphones facilitate shifts in communication landscape for teens. *Pew Research*. Available at http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/.

Morrison, K. (August 11, 2015). "Report: Digital natives do everything from mobile devices. Millennial teens are a digital native generation with a voracious appetite for technology. *Adweek,* Available at: http://www.adweek.com/digital/report-digital-natives-do-everything-from-mobile-devices/

Ng, W. (2012). Can we teach digital natives digital literacy? *Computers & Education*, *59*(3), 1065-1078.

Rubicon Project, "Back-to-School Consumer Pulse" (July 2016). http://rubiconproject.com/insights-report/2016-back-to-school-consumer-pulse/

Shopova, T. (2014). Digital literacy of students and its improvement at the university. *EriE*, 25.

The infinite dial. (2014). Report from Edison Research. Available at: http://www.businessinsider.co.id/instagram-and-snapchat-are-more-popular-than-twitter-among-teens-and-young-adults-sai-2014-3/#.VabHj7VkD94.

United States v. InMobi Pte. Ltd., No. 3:16- CV- 03474 (N.D. Cal. June 22, 2016), https://www.ftc.gov/system/files/documents/cases/160622inmobicmpt.pdf

United States v. LAI Systems, LLC., No. 2:15CV09691 (N.D. Cal. December 17, 2015), https://www.ftc.gov/system/files/documents/cases/151217laicmpt.pdf

United States v. Retro Dreamer., No. 5:15- CV- 02569 (N.D. Cal. December 17, 2015), https://www.ftc.gov/system/files/documents/cases/151217retrodreamercmpt.pdf

Walker, K. L. (2016). Surrendering information through the looking glass: Transparency, trust, and protection. *Journal of Public Policy & Marketing*, *35*(1), 144-158.

Wisniewski, P., Ghosh, A. K., Xu, H., Rosson, M. B., & Carroll, J. M. (2017, February). Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (pp. 51-69). ACM.

Youn, S. (2008). Parental influence and teens' attitude toward online privacy protection. *Journal of Consumer Affairs*, *42*(3), 362-388.