IJoC Communication in Action

How Safe are Safe Harbors? The Difficulties of Self-Regulatory *Children's Online Privacy Protection Act* Programs

BRANDON GOLOB[1]
University of Southern California, USA

Keywords: children online, personal data, online privacy

As communication technology continues to evolve, legal landscapes shift in an attempt to regulate new and emerging media. One pervasive public concern in the digital age is the regulation of online collection of private data. This is by no means a novel concern; for decades academics and practitioners have debated the advantages and disadvantages (and all that falls between) of technological advancement, surveillance, privacy rights, and so forth (Campbell & Carlson, 2002; Dinev, Hart, & Mullen, 2008; Fuchs et al., 2013; Kearns, 1999; Southard IV, 1989). Communication scholarship has been particularly bountiful on these topics because data collection on the Internet is intimately intertwined with questions of communication patterns (Fuchs, 2013; Krontiris, Langheinrich, & Shilton, 2014; Park, 2011). Although concerns over online data collection are varied, the issue of children's information privacy is of particular concern for legal practitioners, communication scholars, and the public at large.

Children are accessing the Internet with increasing regularity and there has been a spike in the number of websites directed at children (Child Trends, 2012). As a result, it has become increasingly difficult to monitor what children access on the Internet and how their data are collected. Children are often the focus of policy efforts because they are a vulnerable population blind to invasions of privacy and the effects of targeted marketing (Chung & Grimes, 2006). Although there have been various legislative attempts to protect children's online information privacy, the most comprehensive legislation in the United States is the Children's Online Protection Privacy Act of 1998 (COPPA). According to the Federal Trade Commission (FTC),

[1] I would like to thank Professor Angela Campbell of Georgetown Law, who helped me formulate the topic for this commentary and provided me outstanding guidance throughout my fellowship at the Institute for Public Representation (IPR). I would also like to thank Katherine Elder, Pamela Krayenbuhl, Jason Smith, and Julian Levitt for dialoguing with me about this project and offering editorial support. Lastly, I would like to extend my gratitude to the Consortium on Media Policy Studies (COMPASS) for funding my work, COMPASS's Summer Fellowship Program Coordinator, Mark Lloyd, for his professional and academic support, and all of my COMPASS colleagues for sharing their inspiring ideas without reservation.

> COPPA imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. (Federal Trade Commission, 2013a)

The FTC is the primary administrator of COPPA, but Section 312.11(a) of the COPPA Rule allows for industry groups or other organizations to apply for a safe harbor status (Federal Trade Commission, 2013b). In short, the safe harbors establish self-regulatory guidelines for meeting COPPA compliance and participants in the harbors are usually subject to these guidelines and disciplinary procedures rather than official FTC protocol. Currently, there are seven active safe harbor programs: (1) the kidSAFE Seal Program, (2) Aristotle International Inc., (3) the Children's Advertising Review Unit (CARU), (4) the Entertainment Software Rating Board (ESRB), (5) Privacy Vaults Online, Inc. (PRIVO), (6) TRUSTe, and (7) iKeepSafe. If a website is part of one of these Commission-approved safe harbor programs, it is deemed automatically compliant with COPPA. At first blush, the growth of self-regulatory COPPA oversight programs is beneficial; presumably, an increase in the number of organizations monitoring and regulating the activities of websites directed at children correlates to an increase in the overall protection of children's online privacy. However, one who dives beneath a preliminary analysis of self-regulatory COPPA oversight programs quickly realizes that little work has been done to assess the effectiveness of such programs. This leads to a clear policy concern: are these safe harbors actually an effective way to protect children's privacy online? It is beyond the scope of this commentary to attempt to measure the effectiveness of the seven safe harbors, but we can begin to analyze why tracking the work of these self-regulatory organizations is a challenge. Reviewing the publicly available information about safe harbors, this commentary critically analyzes the difficulties in assessing the efficacy of self-regulatory COPPA oversight programs and makes policy recommendations for increasing the transparency of how safe harbors review and regulate websites directed at children. The commentary proceeds as follows: (1) an examination of currently existing criticisms of safe harbors; (2) identification of additional criticisms of safe harbors; and (3) recommendations for practices that would help in measuring the role of safe harbors in protecting children online.

Safe Harbor Criticisms

According to the FTC, the safe harbor "provision encourages industry self-regulation, which the Commission believes often can respond more quickly and flexibly than traditional statutory regulation to consumer needs, industry needs, and a dynamic marketplace" (Federal Trade Commission, 2007, pp. 22–23). However, safe harbors have been met with a number of criticisms. As identified by law professor Ira Rubinstein, safe harbors "suffer from two main shortcomings: first, a very low rate of industry participation" and "a lack of regulatory flexibility (all of the approved self-regulatory programs have nearly identical requirements to those of the COPPA statute)" (2010). Following an analysis of these previously identified criticisms of safe harbor programs, this commentary identifies additional difficulties with measuring the effectiveness of COPPA's safe harbor programs.

Low Industry Participation

Tracking the effectiveness of COPPA safe harbors is made difficult by the differences in how safe harbors disclose which websites and technologies they have certified as meeting their self-regulatory program guidelines. For example, the kidSAFE Seal Program offers the clearest way for the public to track the sites and technologies that they have certified by creating a "certified products" directory with an up-to-date list "of kids' websites and apps that have been independently tested and certified to meet a high standard of online safety" (kidSAFE Seal Program, 2011). Similarly, TRUSTe has a searchable database that allows users to enter a site URL to determine which online companies "have earned TRUSTe certification and uphold TRUSTe's high standards for best privacy practices" (TRUSTe, 2014). However, other safe harbors, such as CARU and iKeepSafe, offer little or no information about which sites they certify (Advertising Self-Regulatory Council, 2012; iKeepSafe, 2014).

Without a standardized system for tracking which websites and technologies are certified by safe harbors, it is difficult to quantify what percentage of websites "directed to children under 13 years of age" participate in one of the seven Commission-approved safe harbors. Absent a study quantifying what percentage of children's websites is part of safe harbors, it is still possible to conclude that industry participation is rather low. The universe of children's websites is vast and this number continues to grow, with new websites being created on a regular basis. Bearing in mind that only seven safe harbors exist, each one would have to certify an exponentially greater number of websites in order to substantially impact the percentage of industry participation.

Lack of Regulatory Flexibility

Another previously identified criticism of the COPPA safe harbor programs is that they lack regulatory flexibility. Pursuant to Section 312.11(b)(1) of the COPPA Rule, a safe harbor program must have "program requirements that ensure operators subject to the self-regulatory program guidelines ('subject operators') provide substantially the same or greater protections for children as those contained in Sections 312.2 through 312.8, and 312.10" (Federal Trade Commission, 2013b, n.p.). For example, consider the CARU safe harbor. As noted by Professor Miyazaki, its regulatory guidelines "mirror COPPA requirements, including recommendations for data collection, age screening, verification and parental consent, parental notification, and opt-in and opt-out considerations" (2009, p. 80). In short, the requirement that safe harbors "provide substantially the same or greater protections for children" as those contained within the COPPA Rule has led to little diversity amongst the regulatory requirements of the seven Commission-approved safe harbors. Thus, if the COPPA safe harbors "have nearly identical requirements to those of the COPPA statute," (Rubinstein, 2010) does this defeat the FTC's assertion that the purpose of the safe harbor provision is to help foster a "dynamic marketplace" (Federal Trade Commission, 2007, p. 23)? In other words, is the essence of self-regulation lost if all seven safe harbors have nearly identical regulatory requirements?

Additional Difficulties with Assessing the Effectiveness of Safe Harbor Programs

Although previous literature has discussed some of the major shortcomings of safe harbors, there are additional difficulties with measuring their effectiveness that have yet to be discussed. The remainder of analysis will focus on two central issues: (1) the private nature of safe harbor annual reports to the FTC, and (2) the challenges in tracking constantly evolving "directed at children" websites.

Privacy of Safe Harbor Annual Reports

COPPA Rule Section 312.11(d)(1) required each of the current Commission-approved safe harbor programs to submit a report to the FTC by July 1, 2014 (Federal Trade Commission, 2013b).[2] Pursuant to this section of the Rule, these reports must include

> at a minimum, an aggregated summary of the results of the independent assessments conducted under paragraph (b)(2) of this section, a description of disciplinary action taken against any subject operator under paragraph (b)(3) of this section, and a description of any approvals of member operators' use of a parental consent mechanism, pursuant to Section 312.5(b)(3). (Federal Trade Commission, 2013b, n.p.)

These reports are crucial for determining which websites each safe harbor has certified and whether or not any of those sites have been subject to disciplinary action by the safe harbor. Moreover, if a site has been subject to disciplinary action, these reports would contain details of the action taken. Thus, the information contained in these reports would help increase transparency about the operations of safe harbors and inform analysis as to whether these harbors are effectively protecting children's online privacy. However, these annual reports to the FTC are private and not released to the public. Even organizations working in the field of children's online privacy protection, such as the Institute for Public Representation (IPR), must submit a Freedom of Information Act (FOIA) request to view the reports.[3] Such a veil of secrecy is counterintuitive to promoting public understanding of safe harbor programs and ultimately limits parents' ability to decide whether or not a website is safe for their children.

Defining "Directed at Children" and the Fluid Nature of Digital Media

One of the COPPA Rule's primary thresholds for determining if a website falls under its dominion is whether or not the website is "directed to children." In making this determination, the Commission considers a number of factors, such as its "subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content," and so forth (Federal Trade Commission, 2013b, Section 312.2, n.p.). However, although "directed to children" is statutorily defined,

[2] On July 1, 2014, there were only six Commission-approved safe harbors.

[3] IPR submitted a FOIA request to the FTC but has not received the reports as of the writing of this commentary.

it is often debatable what constitutes a children's website, especially since digital media is constantly evolving. For example, consider Cartoon Network's website. At first glance, Cartoon Network seems to meet the factors to be deemed directed to children, but its privacy policy states that "although children under 13 may visit our Sites, some portions of the Sites may be directed at teens, parents or other adults and collect information only from these older visitors" (Cartoon Network, 2014). Thus, certain content on the site is intended to be "directed to children," while other content is not. This presents an obvious difficulty in deciding whether or not such a site should be certified by a safe harbor as meeting the standards of online safety necessary to protect children's privacy.

Moreover, bearing in mind the constantly changing nature of websites, certification becomes an even more complicated process. Website content changes with the click of a button—one moment a video is posted, the next moment it is removed. This prompts questions as to how long a safe harbor's certification of a website should be valid. What if a website is compliant with a safe harbor's regulations but then changes its content? How do we ensure that after the website receives its seal of approval from a safe harbor it maintains those same practices? Is there consistency in how different safe harbors monitor their sites to ensure continued compliance in the face of constantly evolving digital media?

The Way Forward: COPPA'S Continued Growth

Over the last 15 years, COPPA has been at the forefront of the battle to protect children's privacy online. As communication technology continues to evolve, it becomes increasingly difficult to understand how websites and other technologies collect and use children's data. Thus, Commission-approved safe harbors are expanding in an attempt to monitor websites directed at children and simplify for parents how to tell whether a website meets a high standard of online safety. Although the presence of a safe harbor's certification seal is supposed to signify that a website is safe, it is difficult to assess whether or not safe harbor programs are successful in protecting children from predatory online data collection processes. Much remains to be done to help ensure that children's personal data are safe online, and safe harbors may or may not prove to be the most effective mechanisms for this task. However, at this moment, even assessing their effectiveness is a challenge. Thus, this commentary concludes with suggestions for two practices that would help to measure the role of safe harbors in protecting children online.

Increase the Transparency of the Annual Safe Harbor Reports

As previously noted, each Commission-approved safe harbor is required to submit an annual report to the FTC. Although there are statutorily defined requirements as to what must be included in these reports (a summary of results of independent assessments of children's websites, a description of any disciplinary action taken against any of those websites, etc.), it is not possible to know what the reports actually look like because they are private. This runs counter to the public good that safe harbors are supposed to serve—that is, the protection of children's online privacy data. If the reports were publicly available, this would increase the transparency of how safe harbors operate. People would be able to see which children's websites are following fair data collection practices versus which ones are being subject to disciplinary action for failure to do so.

Moreover, it is possible that some safe harbors are more effective than others. For example, how can it be determined whether the kidSAFE Seal Program does a more effective job of monitoring and disciplining children's websites than the CARU safe harbor, or vice versa? Perhaps parents should place more trust in children's websites certified by certain safe harbors, or perhaps all safe harbors are equally thorough in their certification processes. Analyzing the reports would be a first and crucial step in assessing safe harbors and their internal practices.

Require Each Safe Harbor Website to Have a "Certified Products" List

Currently, there is no standardized system for how safe harbors publicly disclose which websites they certify. While kidSAFE has a portion of its website dedicated to listing all the websites and technologies they have certified, CARU only lists *some* of the clients it represents (Council of Better Business Bureaus, 2014). These differences make it difficult to assess exactly how many children's websites the various safe harbor programs certify. Thus, it should be mandated that each of the seven Commission-approved safe harbors keep an up-to-date list of its certified websites and display that list on its own website. Doing so will (1) standardize how safe harbors keep track of their clients, (2) simplify the search for information about which children's websites are safe, and (3) keep an accurate tally of how many websites participate in a safe harbor program. This small change in how safe harbors present client information will increase public understanding of these safe harbors and their certified constituents, thereby paving the way for other improvements in COPPA's continually growing self-regulatory program.

References

Advertising Self-Regulatory Council (ASRC). (2012). CARU Safe Harbor Program and Requirements. Retrieved from http://www.asrcreviews.org/2011/07/caru-safe-harbor-program-and-requirements/

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online surveillance and the commodification of privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586–606.

Cartoon Network. (2014*).* Privacy policy*.* Retrieved from http://www.cartoonnetwork.com/legal/privacy.html

Child Trends. (2012). *Home computer access and Internet use*. Retrieved from http://www.childtrends.org/wp-content/uploads/2012/07/69_Computer_Use.pdf

Chung, G., & Grimes, S. M. (2006). Data mining the kids: Surveillance and market research strategies in children's online games. *Canadian Journal of Communication*, *30*(4), 527–548.

Council of Better Business Bureaus (CBBB). (2014). Safe Harbor program participants. Retrieved from http://www.bbb.org/council/programs-services/parents-corner1/safe-harbor-program-participants

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance–An empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214–233.

Federal Trade Commission (FTC). (2007). Implementing the Children's Online Privacy Protection Act: A Report to Congress . Retrieved from http://www.ftc.gov/sites/default/files/documents/reports/implementing-childrens-online-privacy-protection-act-federal-trade-commission-report-congress/07coppa_report_to_congress.pdf

Federal Trade Commission (FTC), Children's Online Privacy Protection Rule ("COPPA"). (2013a). Rule Summary. Retrieved from http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

Federal Trade Commission (FTC), Children's Online Privacy Protection Rule: Final Rule Amendments To Clarify the Scope of the Rule and Strengthen Its Protections For Children's Personal Information, 16 C.F.R. §312 (2013b). *U.S. Government Printing Office: Electronic Code of Federal Regulations*. Retrieved from http://www.ecfr.gov/cgi-bin/text-idx?SID=4939e77c77a1a1a08c1cbf905fc4b409&node=16%3A1.0.1.3.36&rgn=div5

Fuchs, C. (2013). Societal and ideological impacts of deep packet inspection Internet surveillance. *Information, Communication & Society*, *16*(8), 1328–1359.

Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (Eds.). (2013). *Internet and surveillance: The challenges of Web 2.0 and social media* (Vol. 16). New York, NY: Routledge.

iKeepSafe. (2014). COPPA. Retrieved from http://www.ikeepsafe.org/privacy/coppa

Kearns, T. B. (1999). Technology and the right to privacy: The convergence of surveillance and information privacy concerns. *William & Mary Bill of Rights Journal*, *7*, 975–1011.

kidSAFE Seal Program. (2014). Certified products. Retrieved from http://www.kidsafeseal.com/certifiedproducts.html

Krontiris, I., Langheinrich, M., & Shilton, K. (2014). Trust and privacy in mobile experience sharing: Future challenges and avenues for research. *Communications Magazine, IEEE*, *52*(8), 50–55.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research*, *40*(2), 215–236.

Rubinstein, Ira. (2010). Guest blog on privacy safe harbors [Web log post]. Retrieved from http://www.futureofprivacy.org/ira-rubinstein-on-safe-harbors

Southard IV, C. D. (1989). Individual privacy and governmental efficiency: Technology's Effect on the government's ability to gather, store, and distribute information. *The John Marshall Journal of Information Technology & Privacy Law*, *9*(3), 359–374.

TRUSTe. (2014). Trusted directory. Retrieved from http://www.truste.com/consumer-privacy/trusted-directory