Must be 13 to Play: Addressing Children Participation in Networked Games

Kara A. Behnke
University of Colorado Boulder,
ATLAS Institute
1125 18th Street, 320 UCB
Boulder, CO 80309
Kara.Consigli@Colorado.EDU

Meg Leta Ambrose
Georgetown University, Department of
Communication, Culture & Technology
3520 Prospect St. NW
Washington, DC 20007
ma1318@Georgetown.EDU

John K. Bennett
University of Colorado Boulder,
Department of Computer Science
1045 Regent Drive, 430 UCB
Boulder, CO 80309
jkb@Colorado.EDU

ABSTRACT
The U.S. Children's Online Privacy Protection Act (COPPA) creates regulatory requirements for website service providers that target children or have knowledge that a user is a child. In this poster, we introduce the state of networked games in the U.S. through the lens of mobile app games, because mobile games represent an "all-ages" environment, are particularly enticing to children, and often depend on personal data-collection to make money. Although some gaming companies take precautions to ensure COPPA compliance, most mobile gaming services furtively avoid COPPA requirements by not inquiring about user age and including a "must be 13 or over" line in their terms of service. This trend in the mobile games industry is problematic, not only because of threat of legal action by federal agencies, but publishers also risk losing potential player audiences such as younger children, since banning users under the age of 13 can be perceived as easier and more cost effect than tackling COPPA compliance. We offer recommendations for how mobile game developers can ensure COPPA compliance more easily and cost-efficiently without disrupting core game design features.

Categories and Subject Descriptors
H5.m. [**Information Interfaces and Presentation**] (e.g., HCI): Miscellaneous.

General Terms
Human Factors, Design.

Keywords
COPPA, children, privacy, policy, apps, mobile gaming.

1. INTRODUCTION
Mobile application games have challenged traditional business models for online users. Mobile "apps" often contain interactive features such as dynamic advertising (e.g., advergaming), links to social media, or the ability to purchase virtual goods through micropayments and micro-transactions. Many apps transmit information from a user's device back to the app developer or, more commonly, to an advertising network, analytics company, or other third party [5].

This raises new concerns for privacy threats related to the disclosure, distribution, collection, processing, and use of data, particularly concerning children and online privacy.

Over 500 million consumers worldwide spent $9 billion on mobile app games in 2013, which is a 32% increase in annual growth from 2012 [7]. This burgeoning industry spurs the interest of many app developers to rely on users' information to streamline revenue. Companies can receive a wide variety of information about users through mobile "device IDs," including data about the device itself and personal data from the user.

Because device IDs are difficult or impossible to change, they can be used by apps, developers, and other companies to compile rich sets of data or "profiles" about individuals. However, many popular educational and gaming apps for children fail to give parents basic explanations about what kinds of personal information the apps collect from children, who can see that data, and what they use it for [5]. This is a direct violation of the U.S. federal Child Online Privacy Protection Act (COPPA).

2. COPPA
Effective since 2000, COPPA [2] protects the privacy of children under the age of thirteen in response to growing concern regarding Internet marketing techniques that target children and depend on massive data collection, processing, and trading without parental participation. It requires parental consent to be obtained in order to collect or use personal information for those users under thirteen. COPPA applies to U.S. and foreign-based commercial websites and online services that are *directed at children* in the U.S. and require them to:

- Provide a detailed privacy policy that describes the information collected from its users, including geo-location information, photos and videos;
- Provide direct notice to parents and acquire verifiable parental consent prior to collection of personal information from a child (by sending/faxing signed printed forms, supplement of credit card numbers, calling toll-free numbers, or forwarding digital signatures through email);
- Provide parents access to child's personal information collected by the online service;
- Include a right to revoke consent, delete information, and prevent further use or collection;
- Limit the personal information collected when a child participates in online games and contests to that which is reasonably necessary to participate in the activities;

- And generally protect the confidentiality, security, and integrity of personal information collected online from children.

COPPA does not apply to general audience websites or online services unless they have *actual knowledge* of children using the site or service or they are "directed to children," which is determined using a number of legal factors including subject matter, visual content, use of animated characters, age of character models, et cetera [3].

2.1 COPPA Enforcement

The FTC can impose civil penalties for violations of COPPA as unfair or deceptive trade practices under § 5 of the Federal Trade Commission Act. COPPA also authorizes state attorneys general to bring actions to enforce compliance with the FTC regulations. As a related matter, U.S.-based sites and services that collect information from foreign children are also subject to COPPA requirements.

COPPA obligations generally remain neglected, unclear, and/or ineffective [4, 5]. The transmission of kids' information to third parties that are invisible and unknown to parents raises concerns about child privacy and the efficacy of COPPA. For example, Xanga was fined $1 million for collecting data because it "knew" user ages through registration [9]. Mobbles Inc., developer of the virtual pet geo-location mobile app game *Mobbles*, allegedly collected children's personal information including e-mail addresses and geo-location without parental consent [8]. After the Center for Digital Democracy filed a complaint with the FTC in December 2012, Mobbles Inc. briefly withdrew the app and put a disclaimer on their product stating that the game was not intended for children under thirteen [8]. However, the description of the game in Apple's App Store and Google Play suggests that *Mobbles* could appeal to younger children, and possibly that *Mobbles* was aware of collecting data "directed at children." Despite the goals of COPPA, sites "intended for older children" are not required to comply with COPPA, leaving those children under the age of thirteen continually at risk.

Nevertheless, some examples of companies that have adequately followed COPPA requirements include Neopets, which requires children under the age of thirteen years to provide parental consent in order to participate in the more interactive or multiplayer components of the site, including forums, multiplayer games and email [6]. Permission to participate in opinion surveys and divulge information to Neopets' third party sponsors is included as part of the consent form, under the claim that these third party transmissions "help keep Neopets free for everyone" [6].

3. DISCUSSION

Mobile app companies frequently use all of the available techniques for targeting adult users to target kids, including geo-location, instant rewards, and in-phone purchases. According to the FTC, 60% of apps transmit device IDs to the developer, with 14% transmitting geo-location and/or phone numbers to the developer or third party [5]. By contrast, only 20% of apps disclosed any information about the app's privacy practice [5]. In addition, third parties that receive information from multiple apps could potentially develop detailed profiles of the children based on their behavior in different apps, yet these third parties frequently do not comply with COPPA requirements [5].

It is clear that more needs to be done to provide parents with more privacy transparency in the mobile app game marketplace. Game designers are legally and ethically responsible for providing safeguards for children's privacy. Even though the general perception is that it is expensive to comply with COPPA and thereby easier to put the clause "must be 13 to play" in the terms of service, there are opportunities for game developers to ethically and economically comply with COPPA regulations without disrupting core game design features and service frameworks.

Increasingly, companies are serving the niche market of making COPPA compliance easy, affordable, and legally safe for mobile game designers and app publishers. For example, AgeCheq [1] is a company that helps eliminate cost and effort for developers and publishers to create their own COPPA compliance suite. AgeCheq delivers COPPA-compliance solutions to verify parents' identities, provide them with easily understandable disclosure statements about child data-collection, and enables parents to easily revoke approval at any time [1]. Moreover, native iOS, Android, and HTML5 software development kits allow an existing mobile app to be retrofitted for COPPA compliance. AgeCheq is one of many companies in this emerging marketplace that enables mobile game developers to effectively and ethically address COPPA regulations with minimized risk and cost.

4. CONCLUSION

Industry appears to have made little progress in improving its disclosures of kids' data usage, whereas COPPA enforcement encourages developers to stay in the dark about the age of their users to avoid fines or to refrain from designing children-specific games altogether. Mobile privacy creates particular challenges but also offers commercial opportunity to help protect children online. Rather than avoid COPPA compliance and risk regulatory fines or possibly lose potential player audiences through the "must be 13 to play" agreement, developers and publishers can utilize existing and emergent COPPA-compliant services to ensure effective and ethical protection for children's online privacy.

5. REFERENCES

[1] AgeCheq. 2013. http://www.agecheq.com/

[2] Children's Online Privacy Protection Act 15 U.S.C. §§ 6501–6506. 1998.

[3] Federal Trade Commission (FTC). 2008. Frequently asked questions about the Children's Online Privacy Protection Rule. Retrieved from http://www.ftc.gov/privacy/coppafaqs.shtm.

[4] Federal Trade Commission (FTC). 2011. Operators of online "virtual worlds" to pay $3 million to settle FTC charges that they illegally collected and disclosed children's personal information. *FTC Press Release*.

[5] Federal Trade Commission (FTC). 2012. Mobile apps for kids: Current privacy disclosures are dis*app*ointing. *FTC Staff Report*.

[6] Neopets parental consent form. (1999-2005). Neopets, Inc. Accessed 15 June 2013, retrieved from http://www.neopets.com/coppa/consentform.phtml

[7] Newzoo Market Research, Inc. 2014. Placing smartphone and tablet gaming in perspective of the total games market. *Newzoo Trend Report: Mobile Games.*

[8] Center for Digital Democracy (CDD). 2012. Request for investigation of Mobbles Corporation's violation of the Children's Online Privacy Protection Act in connection with the Mobbles mobile application. *Institute for Public Representation.* Washington, DC: Center for Digital Democracy.

[9] US v. Xanga.com, Inc., 06-CIV-6853(SHS). S.D. N.Y. 2006.