Case #7a. Internet Companies and Data-gathering from Apps for Children

Synopsis: Case #7a invites you to apply the environmental monitoring framework of Module 7 to judge how internet companies should respond to the NGOs and government agencies who are challenging it on issues related to children's privacy.

According to a 2012 **U.S. Federal Trade Commission (FTC)** report, several hundred of the most popular educational and gaming mobile 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. The apps often transmit the phone number, precise location or unique serial code of a mobile device to app developers, advertising networks or other companies. Government regulators said such information could be used to find or contact children or track their activities across different apps without their parents' knowledge or consent.

The agency reviewed 400 of the most popular children's apps available on Google and Apple platforms, and reported that only 20 percent disclosed their data collection practices. "The survey results described in this report paint a disappointing picture of the privacy protections provided by apps for children," the report said.

The FTC said it was investigating whether the practices of certain apps violated a federal law requiring Web site operators to get parents' permission before collecting or sharing names, phone numbers, addresses or other personal information obtained from children under 13.

The report comes as the agency is preparing to strengthen those protections by requiring site operators to obtain parental consent before collecting many other kinds of personal information from children. But over the last few months, the agency's efforts have met with pushback from Apple, Facebook, Google and Viacom as well as from technology associations and marketing industry groups, who say the agency's proposed solution is so broad that it could inhibit companies from offering sites, apps and other services for children.

In its report, the agency did not disclose the names of apps it found problems with. "We think this is a systematic problem," said Jessica Rich, the associate director of the FTC's division of financial practices, adding that parents should not think "if they avoid certain apps, they are home free."

Representatives of the app industry said they had already been working with app developers to make disclosures about data collection clearer and simpler for consumers. But "the FTC report is a reminder that there is more work to do," said Jon Potter, the president of the **Application Developers Alliance,** an industry group.

The agency's researchers also reported that most apps failed to tell parents when they involved interactive features like advertising, social network sharing or allowing children to make purchases for virtual goods within the app. For instance, researchers found that 58 percent

of the children's apps contained ads, even though just 15 percent disclosed this before download. Moreover, of the 24 apps that stated they did not contain in-app advertising, 10 did contain ads, the report said.

Children's advocates said the report's findings reinforced the need to strengthen online privacy protections for children. The agency has not substantially revised its regulations based on the federal ***Children's Online Privacy Protection Act, or COPPA***, since the law's introduction more than a decade ago. "This makes the case as to why we need major revisions," said James Steyer, the chief executive of **Common Sense Media**, a nonprofit advocacy and education group in San Francisco that focuses on children and technology. "It shows that parents don't have enough information to make good choices."

The timing of the report suggests that the **FTC** is trying to lay the groundwork for its push for broader children's online privacy protections. In interviews, agency officials have said the protections needed to be modernized to keep pace with developments in mobile apps, voice recognition, facial recognition and comprehensive online data collection by marketers. For example, regulators have proposed a longer list of data about children that would require parental consent for Web site operators to collect, including photos, voice recordings and unique mobile device serial numbers. **FTC** officials have also emphasized that they considered the precise location of a mobile device to be personal information whose collection required parental permission. If the agency includes these changes in the final version of its updated regulations, apps would need to get parental consent for a number of data collection practices that are in widespread use.

For example, **FTC** researchers reported that almost 60 percent of the children's apps in the study transmitted a device's ID number, most commonly to an advertising network or another third party. But only 20 percent of the apps disclosed information about these kinds of practices. Regulators said their concern was that marketers or other entities could use these unique device numbers to follow individual children across multiple apps over time, compiling detailed dossiers on their activities. "The transmission of kids' information to third parties that are invisible and unknown to parents raises concerns," the report said.

Although state and federal regulators, along with **industry groups**, have been working to improve disclosures for consumers about how mobile apps collect and use their data, progress has been incremental.

App industry associations have also been working to improve transparency for consumers and parents. For instance, the **Application Developers Alliance**, in a joint project with the **American Civil Liberties Union** and other advocacy groups, has created prototype disclosure notices that apps could voluntarily display before consumers download them. "I think the app industry continues to work with our members, companies and consumer groups to identify and eventually implement more effective ways of communicating with consumers," said Mr. Potter, the president of the app developers' group.

Ms. Rich of the FTC said she hoped the agency's report would "light a fire" under such efforts. She added that the agency intended to conduct studies regularly on the children's app market and publicly report its findings.

A version of this article appeared in print on December 11, 2012, on page B1 of the New York edition with the headline: "Children's Apps Fall Short on Parental Disclosure, U.S. Says."

Protection of Children Information in Europe

With the recent adoption of the *General Data Protection Regulation (GDPR),* the **European Union (EU)** assigned a prominent role to parental consent in order to protect the personal data of minors online. For the first time, the GDPR requires parental consent before information society service providers can process the personal data of children under 16 years of age. This provision is new for Europe and faces many interpretation and implementation challenges, but not for the US, which adopted detailed rules for the operators that collect personal information from children under the *Children's Online Privacy Protection Act (COPPA)* almost two decades ago.

For details on the GDPR treatment of children's data, see **Volume 26, 2017 - Issue 2, Milda Macenaite & Eleni Kosta, "Consent for processing children's personal data in the EU: following in US footsteps?" Pages 146-197 | Published online: 10 May 2017**

https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096

Below is some additional information from that article:

Children are actively present online at an ever-younger age. It is estimated, that globally one in three internet users are under the age of 18. Online, children not only enjoy exciting opportunities of playing, creating, learning, self-expressing, experimenting with relationships and identities, but are also disclosing increasing amounts of their personal data. Ubiquitous computing and the increasing datafication of everything is seen as enhancing online privacy risks, such as commercial exploitation and misuse of personal data, profiling, identity theft, the loss of reputation and discrimination. For example, as the consequence of dataveillance practices via wearable and mobile devices, social media platforms, and educational software, 'children are configured as algorithmic assemblages with the possibility that their complexities, potentialities and opportunities may be circumscribed'. In addition, due to their particular behavioural characteristics, emotional volatility and impulsiveness, children (especially teenagers) are seen as being more vulnerable in comparison to adults online. Young people are sometimes at risk not because their brains are different, but because they have not had the experience or opportunity to develop the skills and judgment that engagement in those activities and experiences supply. They may be less capable of evaluating perilous situations and can be more easily misled, given their lack of awareness vis-à-vis the long-term consequences of their virtual actions. The specific developmental features of children might be easily exploited by online marketers who collect personal data and employ special techniques such as 'real-time bidding, location targeting (especially when the user is near a point of purchase), and "dynamic creative" ads tailored to their individual profile and behavioral patterns'

Empirical studies show that privacy risks are common on the internet. For example, according to the empirical data of the EU Kids online, 9% of children aged 11–16 in Europe have experienced personal data misuse online. In the same vein, adults widely support the introduction of the special data protection measures for children. According to an Eurobarometer survey, 95% of Europeans believed that 'under-age children should be specially protected from the collection and disclosure of personal data' and 96% thought that 'minors should be warned of the consequences of collecting and disclosing personal data'. Given these online risks and public concerns, there have been increasing calls from policy-makers and academics to transform children's rights, in particular the rights guaranteed by the UN Convention on the Rights of the Child (UN CRC), to cater for the 'digital age'. Among the rights to provision and participation, the UN CRC recognises children's rights to protection, including a specific protection against arbitrary or unlawful interference with children's privacy, and unlawful attacks on their honour and reputation

Yet, protection of informational privacy in the European Union (EU) has been designed for 'everyone', conflating adults and children in one single group of data subjects. Since 1995, minors are covered by the age-generic data protection provisions provided by Directive 95/46/EC with no special focus on the processing of children's data. The newly adopted *EU General Data Protection Regulation* of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The GDPR explicitly recognises that children need more protection than adults. As explained by Recital 38 of the GDPR, children merit special protection as they 'may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data', especially online. To provide such special protection, the GDPR has introduced far-reaching changes in relation to the processing of minor's personal data online, such as child-appropriate information, a stricter right to erasure, and stronger protection against marketing and profiling. Most importantly and controversially, in cases when the processing of personal data of children takes place on the basis of consent Article 8 of the GDPR has established a parental consent requirement before the offering of 'information society services' directly to children under the age of 16 (unless a lower national age threshold between 13 and 16 applies).

Being new, the GDPR's parental consent requirement remains unclear and faces many practical implementation challenges. However, in the US since 1998 the Children's Online Privacy Protection Act (COPPA) has provided detailed rules for the operators of online services directed towards children that collect (or have actual knowledge that they collect) personal information from children. As the GDPR has been partially inspired by COPPA, US experience could inform the debate in the EU over the new data protection challenges related to children's consent in relation to online services. Thus, the aim of this article is to critically assess the provisions of the GDPR related to the consent of minors, and make a comparative analysis with the requirements stipulated in the US COPPA in order to identify pitfalls and lessons to be learnt before the new rules on the consent of minors in the EU become applicable.

Questions:

1. **(2) What should Internet Companies' policy be regarding protection of children from data abuse? (maximum length 100 words)**
2. **(2) Identify two issues, two organizations, and two internet sites that Internet Companies should be monitoring to make sure it stays ahead of the data abuse issue so that the issue does not present major problems for the companies. Segregate your answers and be as specific as possible in each category:**
   a. **Issues**
   b. **Organizations**
   c. **Internet sites**

   (no maximum length for Q2)

NOTE: "Be as specific as possible in each category" means precisely that. I expect you to name specific issues, organizations, internet sites and print or electronic media! In previous classes, many students tended to give generic answers!

3. **(2) Choose 1 "signal" in the Internet Companies environment that you would categorize as particularly "strong?" If you cannot identify one strong signal, choose a weaker signal and assess its strength. (explain you assessment using the 3 prescribed metrics for measuring the strength of signals—strength, timing, and potential impact.)**

(maximum length for Q3 60 words)

(2) What should Internet Companies's response be to that signal?

(maximum length for Q4 60 words)