Part 3

No Child's Play: Putting Children in Harm's Way

Chapter 6:
Ethics of Business of Social Media and Gaming

Ajay Kumar Sinha[i]

The Web of Social Media

On July 19, 2019 the Indian media widely reported the move by the Ministry of Electronics and Information Technology, Government of India, to seek answers from Beijing ByteDance Technology Co Ltd., owner of the popular Chinese video app TikTok, to a voluminous list of 24 questions.[ii] The questions ranged from alleged unlawful usage of TikTok by children to availability of content that is obscene and anti-national. The Ministry also enquired whether TikTok restricts usage of the app among children, or those below the age of 18 years through its 'age gate' mechanism, and if the mechanism can be made applicable for users who are already registered. The government sought detailed responses on the Company's policies with regard to obscene content available on the platform, about the preventive and corrective measures ByteDance had taken to ensure that such content does not appear on the platform and whether it has taken significant steps to sensitise children and parents to ensure safe use of the platform and 'avoid any addiction to the application' by the younger generation.

It is important to know that ByteDance is one of the world's most valuable start-ups, even though both TikTok and Helo are not offered in their home-market China. The Company, which has seen blistering growth in India, was also questioned on data localisation and whether the Company was in compliance of the Information Technology (Intermediaries guidelines) Rules, 2011, and other Indian laws apart from the IT Act.

This questioning of ByteDance by the Ministry is quite noteworthy as TikTok is not the lone application that is in violation of the UN conventions, laws, policies and ethical norms of the society. There are numerous social media and online gaming companies that are operating in India who pay scant regard and consideration to the effect content produced and/or hosted by them, or on their platforms, has on children and young people. Such companies are in serious need of reform and restructuring of standards and mechanisms, so they are in compliance of the standards of children's rights to privacy, safety, health and well-being as they are espoused in the Constitution of India and the United Nations Convention on the Rights of the Child (UNCRC). These companies seem to be doing business of their products and services in the Indian market while being completely oblivious to their social responsibilities of protecting and promoting peace, harmony, non-violence and preventing sexual abuse and exploitation, addiction and other practices like gambling, which are harmful for the society in general and children in particular. It is a matter of both social responsibility of the business and of business ethics. A business that thrives on and flourishes from causing harm to its clients, buyers and users is unethical and criminal.

Recently, there was also news of a ban on the PUBG mobile game, one of the most popular mobile games in India, in Gujarat and arrests of some young adults who were playing the game.[iii] This made the whole nation take notice of a phenomenon that a majority of the population is facing but for which there is very little attention from – (a) law and policy makers, (b) teachers and schools and (c) parents and guardians.

Tencent, the makers of PUBG, have received flak for not doing enough to prevent children from getting 'addicted' to the game and affecting their overall behaviour due to the promotion of gun violence in the game. The ban and news

around it has triggered a national conversation around regulating online gaming in India. When we look around and talk to people in general, almost everyone is facing the problem of people spending more than the desirable amount of time looking into the screens of their smart phones. However, very few understand the reasons behind the malaise and what could be the possible solution.

What needs to be discussed and understood is the lack of laws and regulation surrounding gaming in India, the lack of any law requiring compliance with international guidelines and rating systems and the nuanced difference between – (a) an online game being objectionable due to its violent and sexually inappropriate content and (b) the addictive nature of the online game.

Additionally, the differential adverse impacts of 'Violent and Sexually Inappropriate Content' and 'Addictive Nature' of online games on children also need discussion and solution. There is a need to understand these phenomena that are multi-dimensional and which permeate and flourish in an environment lacking any central administration of the Internet. This allows organic growth of the network, as well as the non-proprietary nature of the Internet protocols, which encourages vendor interoperability and prevents any one company from exerting too much control over the network. This reality of the Internet also hinders the government from intervening with any real authority.

The Modus Operandi of Online Gaming and Social Media Companies

One often wonders whether we own our technology, or our technology owns us. Our use of technology changed from a tool we want to use into a tool we must use. The devices and services have crept further into our personal lives, demanding an increasing amount of our attention and engagement.

But, why do we behave the way we do? Why are we always hooked on to digital devices? Is there someone who is planning and plotting to keep us using more and more social media and online gaming? We need to understand that most of the content we consume online is also watching us, recording us, and building a digital version of us. That digital version of us is quite valuable. So, the true owners of technology need us to be as engaged in the technology as possible. Because **WE** are the product they are selling. Our digital identity and our online behaviour (tracked by algorithms of the digital media companies) are the products.

We binge on a lot of things in the modern world – TV shows, video games, food, alcohol, social media, and all the other menu items available in our modern-day dopamine buffet. It is great in the sense that we've never had so many options for enjoying life, but it also means that the companies responsible for serving up the feast are highly incentivised to keep us logged in to using their online gaming and social media applications.

As mobile games and in-game payment models become the new norm in video gaming, we are in for a whole new generation of carefully-tailored compulsion loops that most people will find hard to resist. Who likes saying no to some free dopamine? As game consumers, if one finds a game using compulsion loops without a satisfying end in sight, the game may be taking more from the player in terms of time than what they are getting back in terms of enjoyment.

Persistent identifiers are the main fuel of the online tracking industry. These are used by the companies to gain insights into the websites we visit and the apps we use, including what we do within those apps, mostly in violation of the laid down policies. A persistent identifier is just a unique number that is used to either identify us or our devices. Examples of persistent identifiers used in real life are our Social Security numbers and phone numbers. Web Cookies use persistent identifiers to identify us across websites and apps.

On our mobile device, there are many different types of persistent identifiers that are used by app developers and third parties contacted by those apps. For example, one app might send an advertising network our device's serial number. When a different app on the same phone sends that same advertising network our device's serial number, that advertising network now knows that we use both apps and can use that information to profile us. This sort of profiling is what is meant by 'behavioral advertising.' That is, they track our behaviour so that they can infer our interests from the behaviour pattern, and then send us ads targeted at the inferred interests.

In 2013, with the creation of the 'ad ID', both Android and iOS unveiled a new persistent identifier based in software that provides the user with privacy controls to reset that identifier at will (similar to clearing cookies).

Of course, being able to reset the ad identifier is only a good privacy-preserving solution if it is the only identifier being collected from the device. Imagine the following situation:

1. An app sends both the ad ID and the IMEI (a non-resettable hardware-based identifier) to a data broker.
2. Concerned with her privacy, the user uses one of the above privacy settings panels to reset her phone's ad ID.
3. Later, when using a different app, the same data broker is sent the new ad ID alongside the IMEI.
4. The data broker sees that while the ad IDs are different between these two transmissions, the IMEI is the same, and therefore, they must have come from the same device. Knowing this, the data broker can then add the second transmission to the user's existing profile.

In this case, sending a non-resettable identifier alongside the ad ID completely undermines the privacy-preserving properties of the ad ID; resetting it does not prevent tracking. For this reason, both iOS and Android have policies that prohibit developers from transmitting other identifiers alongside the ad ID. For example, in 2017, it was major news that Uber's app had violated iOS App Store privacy guidelines by collecting non-resettable persistent identifiers. Tim Cook personally threatened to have the Uber app removed from the store. Similarly, Google's Play Store policy says that the ad ID cannot be transmitted alongside other identifiers without users' explicit consent, and that for advertising purposes, the ad ID is the only identifier that can be used. However, there still continue to be lots of violations by the online gaming and social media industry (read online tracking and profiling industry!).

The Digital Space: Are Children Safe?

In the case of children, one of the most critical issues with digital technology is the impact on their digital identities over their life course. This digital identity is extremely dynamic and keeps changing and updating as the software platforms are constantly busy in the acquisition and processing of information (updates, photographs, additional information). The most significant player in the construction of the digital identity is the host of online gaming and social media services that collects and utilises the personal data, more often than not for economic purposes. Within this context, the data that is collected from and of children may, at any uncertain point in the future, be utilised and analysed by indeterminate algorithms, for indeterminate clients, to create digital identities or to perform any operation in the digital space, of which the individuals/children are unaware and have no control.

Today, the following cyber-risks gravely affect children worldwide:

1. Digital misinformation (violation of Article 17 – Access to Relevant Information and Media)
2. Cyberbullying (violation of Article 19 – Protection from all forms of Violence)

3. Online grooming (violation of Article 11 – Kidnapping)
4. Technology addiction (violation of Articles 19, 31 – The Right to Relax and Play)
5. Privacy invasion and hacking (Articles 8, 16 – The Right to Privacy and Preservation of Identity)
6. Exposure to violent and inappropriate contents/contacts (Article 17, 19, 34 – The Right Against Sexual Exploitation) and
7. Online radicalisation and trafficking (Article 35 – The Right against Abduction and Trafficking)

Articles 3 (best interests of the child), 4 (protection of rights) and 6 (survival and healthy development) clearly state that every measure must be taken to ensure the respect, protection and fulfilment of children's rights by governments and all other stakeholders. Thus, there is an urgent call for us to work together to put our children first and to reshape the digital ecosystem.

So, in a nutshell it is the online tracking industry that runs on a hacked dopamine reward system. It thrives on – (a) keeping us logged into online video games and social media more and more, and (b) making us lose our agency ('agency' means independence of our thought and decision making). The companies earn money on the basis of these two hard realities and their business model is anything but ethical.

There is a need for companies to be brought to a discussion board by the Government of India and find a way forward so that the profit motive does not completely takeover societal and human concerns. After all, the companies and businesses will also survive and flourish when the humanity and society survive and flourish. A short term and short-sighted profit motive will spell doom to all of us.

i. Forum for Learning and Action with Innovation and Rigour (FLAIR)

ii. India Today Tech (2019) TikTok at risk of ban in India? ByteDance says working with govt, assures users everything is alright, India Today. Available at: https://www.indiatoday.in/technology/news/story/tiktok-ban-in-india-bytedance-working-with-govt-1570844-2019-07-18

iii. https://www.indiatoday.in/technology/features/story/10-arrested-for-playing-pubg-in-gujarat-what-was-govt-warning-why-arrests-and-everything-you-need-to-know-1477832-2019-03-14