Policy Platform

About us: *Design It For Us is a youth-led coalition advocating for safer online platforms and social media. We aim to drive and achieve key policy reforms to protect kids, teens, and young adults online through the mobilization of youth activists, leaders, and voices.*

INTRODUCTION

The online ecosystem can be a productive and positive place. We benefit every day from the creativity it fosters, the communities it strengthens and the vast personal and intellectual growth it enables. But the unchecked, profit-driven mechanisms employed by Big Tech on social media and online platforms have caused immense and unnecessary harm. Big Tech has addicted and exploited our generation. Our mental, physical and emotional wellbeing is at stake. Accountability is long overdue.

VISION

We deserve products and policies that respect our privacy and safety, and are designed with us in mind. As digital natives, we demand a safer environment in which we can continue to grow and thrive. We don't want to neglect social media - we want to make it better.

At this urgent moment, when the mental health and wellbeing of our youngest generations are at an all time low, taking productive action can have a ripple effect – making urgent and meaningful changes now can drive momentum for continuous reform. Our generation and those to follow deserve to know that our wellbeing is a priority, not an option. A safer online environment for all can and should be achieved. Our policy platform puts forth key principles that we strive to uphold in our support for legislation and policy meant to best protect kids, teens, and young people online today. As technology and the online ecosystem continue to change, we will update these principles to meet each moment.

To achieve that vision, Design It For Us supports policy that adheres to 5 key principles:

1. The responsibility of safety rests on Big Tech.
2. Address the business model.
3. Provide and prioritize user agency.
4. Algorithmic accountability.
5. Data use, minimization, and user control.

I. **The responsibility of safety rests on Big Tech.** Big Tech companies are the designers, creators and manufacturers of product features that have been proven harmful to kids, teens and young adults. Tech policy should put the responsibility of safety on Big Tech – not kids or parents – to make their products safer.

A. Policies that hold Big Tech accountable should **require platforms to uphold the highest safety standards by design and by default**. Like manufacturers do for cars and seatbelts, platforms should be required to be safe upon entry, so that users can safely experience the services provided by the platform. Harmful design features (as included in Appendix 1), like infinite scroll and autoplay, should be turned off for users under 18 by default.

B. Policies that hold Big Tech accountable **do not prohibit or restrict kids, teens and young adults from using social media or accessing the internet** – we should not be punished for design choices we did not make.

C. Policies that hold Big Tech accountable **do not require parent or guardian consent for kids and teens age 13 and over to access sites and platforms**. Not all parents have the time, capacity, or knowledge to know what happens online, or how to set safeguards or otherwise get involved. Some kids and teens don't have parents or adults who can serve in this capacity, or who have their actual best interests in mind. If kids and teens need to rely on parental figures to gain access to online communities, some will lose crucial access and information. This gap not only fails to keep all kids safe, but also would have a disproportionate impact on young people from marginalized communities.

D. Policies that hold Big Tech accountable **do not enact *arbitrary* user-facing restrictions, including: curfews and bans of usage**. We are digital natives – we will always find ways to be connected online. Rather than attempt to prevent us from accessing platforms at all, effective legislation should make social media and online platforms safer for use. Restrictions placed on the user – instead of adjustments to the design of the platforms themselves – allow Big Tech to maintain their status quo and continue designing products with harmful features.

II. **Address the business model.** Proactively and directly regulate surveillance capitalism employed by social media companies and online platforms to exploit the wellbeing of users for profit. Centralize privacy as a fundamental and essential value, not profit.

A. Policies that protect users from surveillance capitalism should **ban the use of surveillance advertising and targeted advertising for kids, teens and young adults**. Surveillance advertising is the core profit-driving mechanism that advertisers and companies like Meta, Google, and TikTok use to extensively track and profile individual groups, and microtarget them based on their relationships, behavior and identity. This mechanism actively curates what we see online without our consent and intentionally serves content that keeps each individual user addicted, in order to serve more ads and retain user time. This design mechanism amplifies hate and manipulates our online profiles for profit.

B. Policies that protect users from surveillance capitalism should **require platforms to uphold the highest privacy standards by design and by default**. Companies and platforms should not be allowed to share or profit from the distribution of personal data, and should be restricted from the ability to unnecessarily collect or use personal data beyond what is necessary at the point of service.

C. Policies that prioritize user privacy over profit driven tactics **should not require the submission of additional information to a platform or site to ensure age-appropriate safety mechanisms are in place**. Where age assurance is not already possible, platforms should default to the highest safety settings. Because companies, platforms and social media products are fundamentally profit-driven, they should be restricted from any unnecessary access to users' personal information.

D. Policies that prioritize user privacy over profit-driven tactics should **restrict the use of all deceptive practices and tools to collect data without notice or *informed* consent**. Companies and platforms regularly opt to apply default cookies and hidden harmful features that users are unable to consent to or reject upon entering a site or joining a platform. For example, companies like Meta and Google have been found to routinely attach personalized cookies to online users to track and distribute personal data about its users for their own business purposes. Moreover, when unrestricted, platforms and companies can and will innovate new features meant to collect data to be shared with advertisers.

III. **Provide and prioritize user agency.** Kids, teens and young adults must be able to make their own choices about their online experiences. It is critical to give power to users to co-create an online environment that will allow us to reap the benefits the internet has to offer.

A. Policies that prioritize agency and choice should **provide extensive user-end customization of safety features, with the default set to the strongest safety and privacy options**. We cannot approach tech policy with a one-size fits all assumption. Every user is different and every user's experience on every platform is different. Upon entering any platform, users should be able to adjust their safety settings at any point. When a platform's safety features are safest by default, a user can navigate how to customize their experience while in the safest environment, and not the other way around.

B. Policies that prioritize agency and choice must **give users the ability to protect their personal profiles by default**. Users should have full ownership of what anyone can see or have access to on social media sites and online platforms. Predators, bullies and other nefarious users should not be able to have an undeterrable ability to view personal details about a user. Rather, users should have the option to turn off some or all profile protections as preferred and block predatory accounts.

IV. **Algorithmic accountability.** Deprioritize algorithmic and engagement-based mechanisms and hold companies and platforms accountable for manipulative algorithmic features that amplify harmful content and addict users.

A. Policies should **prohibit the use of dark patterns and manipulative design mechanisms created to deceive and drive engagement-based profit**. Techniques employed by platforms, such as misdirecting users and tricking users into unknowingly sharing more information than they intended, are purposeful tactics designed to collect additional data and profit by manipulating users. These are intentional privacy-evading policy choices that can and should be prohibited in order to prioritize user privacy over profit. Platforms should be accountable for building products that do not rely on profit-motivated engagement or patterns explicitly designed to manipulate users and capitalize on personal data.

B. Policies should establish **safety standards that are specific to platforms and websites at the point of design**. Policies should not regulate a user's experience at the point of product use, only at the point of design and production, wherein a company has near infinite freedom and resources to proactively design products with user safety as its only priority. **After the point of production, efforts to regulate the user experience become a user's burden.** Moreover, algorithmic designs are already found to be flawed and biased, perpetuating negative and harmful sentiments towards marginalized communities. Platforms should be prevented from continuing to implement design features that actively promote harm.

V. **Data use, minimization, and user control.** From the ideation to the production to the use of a product or platform, users should have the comprehensive and unconditional ability to have visibility into and control of their personal information at any moment or point of use.

A. Policies that guarantee data minimization and transparent user control should **require that companies, advertisers and platforms use concise, clear, legible and accessible terms to describe exactly how personal information is used, stored, and by whom**. The veiled, concealed and most often absent practice of disclosure by platforms and companies is harmful and manipulative. Most users will not and should not need to know how to read and interpret legalese – language should be upfront, easy to understand, and convey all possible details about the interaction between a user, their data and any platform.

B. Policies that prioritize data minimization and transparent user control **should enable interoperability**. Companies should make available easy-to-use, comprehensive tools allowing users to download their personal data and information. Users should have control over their own data across platforms, and have the ability to block a platform's ability to retain or preserve personal data unless given express permission.

C. Policies that prioritize data minimization and transparent user control should **require that platform producers and companies disclose what data capture mechanisms will be used before users join a platform**. Companies should be required to share publicly what mechanisms will be used as part of or in partnership with advertising and data capture tactics before a user creates an account. Users should have the right to assess the tactics and choose for themselves if it's something they will opt-in to. This would also incentivize platforms to competitively innovate towards safer tools and mechanisms that would positively shape user experiences.

D. Policies that prioritize data minimization and transparent user control should **require that users have the option to be notified when their data is being viewed or used. Simultaneously, users should be able to comprehensively and quickly delete their data from a site or platform they no longer wish to use, especially when a user deletes an account**. Users should have complete visibility into where their data goes – without this level of transparency, platforms can manipulate and usurp data for their own profit.

E. Policies that prioritize data minimization and transparent user control should **require that users under the age of 13 be notified when a parent, guardian or approved adult views a user's profile**. For the youngest users, having support from a supervisory figure can be beneficial, however, unchecked access to a young user's profile can often be an invasion of privacy. Especially in households where a young user and their parental figure may not agree or align on key identities, ideologies or lifestyles, parents should not have undeterred access to a young user's profile.

F. Policies that prioritize data minimization and transparent user control should **require that companies and platforms provide researcher access to data from online platforms** – not user data – to foster further understanding of the impact and harms of design features that are in effect and likely to be in effect. Unlike the existing, unchecked, black box nature of company data, transparent access to company research should also incentivize competitive innovation towards the safest and most private practices.

CONCLUSION

The internet is responsible for revolutions; for bringing family and community together; for educating people across the globe. It must be clear – the internet is not inherently a bad place, and while it does require regulation – it shouldn't be seen as an enemy. When we think about how to tackle this intergenerational challenge, we must acknowledge that there is a gaping distinction between the potential for good online, and those who nefariously manipulate their unregulated access to personal information. In spite of the fact that the tech industry and our society are driven by profit, we must remember that *humans* above all will feel the impacts of our decisions, or our inaction. People using digital platforms – especially children, teens and their parents – should not shoulder the sole responsibility of ensuring privacy and safety, nor experience the existing and future harms of inaction. Rather, we must enact accountability that is long term, sustainable, and reinforces the vast possibilities of good that is our virtual global community.

APPENDIX 1 [1]

Harmful design features include:

- ***Auto-play*** - a feature that enables videos to automatically continue playing without manual intervention. Videos that are automatically played are often recommended by platforms based on the current video and watch history of each user. Auto-play provides a continuous supply of dopamine, making platforms and videos more addictive and harder to cease using.

- ***Infinite scroll*** - content feeds that continuously populate with new content, creating an endless inventory of content that a user can scroll through. Infinite scrolling provides a continuous supply of dopamine, making platforms more addictive and harder to cease using.

- ***Collection geo-location information*** - the digital capture of the real-world location of a user, which is done by generating their coordinates through the triangulation of data derived from GPS, IP, MAC, RF and EXIF data. The collection of geo-location data, especially for minors, is dangerous, and could lead to harm by strangers on and offline.

- ***Retention of geo-location information*** - the practice employed by platforms and services of saving or holding collected geolocation information beyond the point of service. Retention inherently gives a platform control over a user's location data, which presents a persistent likelihood of harm, especially for minors, on and offline.

- ***Hyper-personalized algorithms*** - recommendation systems that use personal data like age, gender, location, search history and online behavior to drive acutely targeted videos, images and links on platforms meant to align with known data points about a user. Hyper-personalization takes advantage of data collected with and without consent, such as data collected by third party cookies. The consistent receipt of content that a user is predicted to enjoy supplies dopamine, making platforms more addictive and harder to cease using.

- ***Public display of engagement and engagement metrics*** - publicly viewable metrics that show how other individuals interact with a user's content. Metrics include "like" counts, "view" counts, comments and comment counts. These engagement metrics have a neurological impact on users, simulating a social reward that, by nature, is a necessity to humans. This makes platforms more addictive.

- ***Nudges*** - system design features that encourage a user towards a certain behavior, direction or choice. Nudges create social pressures that undermine wellbeing, promote stress and social anxiety, and make platforms more addictive.

[1] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6679162/