Youth Criminal Conduct in Gaming

Workshop Learnings and Outcomes Report

Hosted by the Fair Play Alliance
30 gaming companies in attendance
Workshop Date: March 15, 2022
***
All discussions and insights held to Chatham House Rules

Executive Summary

Youth criminal conduct in gaming is a serious issue that can negatively impact the perpetrator and their future prospects, increasing the likelihood that their behavior escalates to more serious crimes. Such conduct also directly harms gaming companies, impacting the bottom line and putting undue stress on employees. These behaviors, when left unaddressed, serve to normalize this conduct while those exposed to transgressions in the ecosystem may be more likely to themselves participate given a future opportunity.

While the causes behind youth criminal conduct in gaming are manifold, it can largely be summed up as the perception of such transgressions as “not a big deal”, socially advantageous, or simply fun. The cognitive immaturity of youth further leaves them ill-equipped to assess consequences and rendering them more vulnerable to bad actors who may seek to exploit minors.

There are many challenges to addressing such conduct: Variations in youth’s developmental age or overall maturity can make it difficult to develop effective strategies. As well, the reinforcement of behaviors in part due to their impact on one’s perceived social status can be difficult to overcome–fitting in as a youth is a critical desire. The prevalence of resources online on how to participate in these transgressions also means a child typically has easy and often unsupervised access to problematic materials; caretakers often do not reasonably have the resources or capacity to adequately monitor or intervene. Game companies and law enforcement are often not set up for successful collaboration, while the decentralized nature of gaming can create difficulties for understanding jurisdiction.

Furthermore, companies themselves may sometimes find they face inconsistencies within their own studios around the question of when or how to shut down a profitable streamer who may not be setting an ideal example. Even when the answer is clear, it is not always feasible to detect and address all such sources given the vastness of the internet.

As a result of this workshop, several recommendations have been put forth to help address issues of youth criminal conduct in gaming:

- Increase the amount of youth-focused education and modeling of healthier behaviors (while identifying and deplatforming unhealthy models). Leverage games and gaming media as a means to reach youth in a more relatable way.
- Focus on more accessible and appropriate means for supporting caregivers, being mindful of variations in tech literacy. As well, the parental controls provided by gaming companies and platforms are often opaque and difficult to use effectively and improvements should be prioritized.
- Consider the opportunities presented by the design of games themselves, and how they can promote healthier behaviors in the first place. There are also opportunities to expand enforcement strategies within games with an emphasis on education.
- Develop collaborative strategies between game companies and law enforcement globally, with a focus on the needs and challenges faced by each type of organization and how they can better support one another in this endeavor.
- Create resources on the best practices that emerge from the above to share these learnings equitably across the games industry (and beyond).

In the short term, we recommend convening around a series of more targeted, action-oriented discussions to start to explore next steps on the above.

Background

The Fair Play Alliance (FPA) recently has been addressing child safety–how to keep children safe in our games and online–with particular focus on protective practices for children and platforms to employ. There are instances, however, where youth (i.e., those who are still undergoing cognitive development; those younger than 25 years old) are the “bad actors” engaging in disruptive and sometimes even criminal behavior (see **Glossary of Terms**).

As the industry moves towards more robust practices for child safety in gaming, we are opening up the discussion on juveniles/youth as perpetrators of criminal behavior. It is worth noting that youth are not always aware that their behaviors on and across the platforms they engage with are illegal or harmful. Furthermore, there is a greater vulnerability among youth who may lack the skills to adequately assess the repercussions of their actions or who may be led astray by other influential actors in the ecosystem.

This workshop invited the U.S Department of Justice (DoJ) as guests to share their knowledge. The session treated FPA members as stakeholders to better understand the scope of youth criminal behavior in gaming to align on where to best put our efforts as an industry.

Workshop objectives

- **Understand the impact** of criminal conduct on the gaming industry
- **Share what we know** about youth engaged in criminal conduct on gaming platforms, the business context around criminal behavior
- **Identify opportunities** for better ways to address criminal conduct in gaming, including:
    - How we can engage with players and steer youth productively, such as redirecting bad actors
    - What the gaming industry needs from the DoJ or law enforcement to support these efforts

Problem space

Games present an opportunity to connect with youth in intentional ways and provide an avenue to become familiar with new ways of thinking, social interactions, and emerging technologies. As youth explore gameplay, however, they may engage in **criminal behavior** as they learn from peers and online resources including how to hack, employ distributed denial-of-service (DDoS) attacks, or swat other players. These behaviors may not always be conducted with an appreciation of the consequences or even be intentionally malicious–it is normal for youth to push the limits of their own understanding and the technologies to which they're exposed. Nonetheless, these actions are violative, can cause extensive damage, and can set youth on a path to a criminal record and even worse crimes, making them hard to ignore.

The U.S. Department of Justice is focused on addressing these criminal behaviors, with a large focus on preventative measures such as outreach and education. In particular, there is interest in identifying ways that we might leverage the space of games to help prevent youth from becoming perpetrators of criminal behaviors online in the first place.

This workshop aimed to understand the intersection of youth criminal conduct and the gaming space, and whether the Fair Play Alliance membership might have a perspective. During the workshop, we were operating on the following working assumptions:

- We did not presume that the FPA membership had an explicit interest in the government helping with the problem of Youth Criminal Conduct in gaming. As such, all discussion was exploratory on the membership's attitudes and needs.
- Though the intersection of games and youth crime is the primary topic of discussion, we do not assume or even propose a causal or correlational relationship. Rather, we look to gaming as an avenue to reach and engage a population that may be at increased risk of criminal conduct, with games and game platforms as potential opportunities to steer them away from such behavior.

The following sections of this document summarize the discussion from the workshop. All discussions were held to Chatham House Rules, where the membership is allowed to discuss the themes and topics, but not to attribute discussion back to any individual, company, or institution.

Understanding what's happening in gaming and why

The first part of the discussion was dedicated to understanding the intersections of youth criminal conduct and gaming, including what we know about the motivations and behaviors of youth that execute such behaviors, the types of criminal behaviors seen today.

Who and why: Context of behaviors and motivations

While some of the people conducting criminal behavior in games may have malicious intent, it is not true that they all do. Instead of thinking about these youth in a binary as either bad actors or good actors, it better serves the industry to understand their motivations and incentives as the behavioral drivers that can be targeted with design or education. As such, values and norms set for players by system design may be a key component to preventing criminal conduct sustainably.

Social motivations

One of the primary motivators for youth to conduct criminal conduct in gaming is social status and social norms. As children develop, they grow in curiosity and are learning about social boundaries–what is and isn't acceptable within a set of social norms. Children may pursue criminal conduct to increase their social status, to be seen as "cool", in a misdirected expression of emotion, or to gain notoriety.

By identifying vulnerabilities in games and online systems, young people showcase their creativity and gain a sense of power by doing so. Some children that have conducted these behaviors do so to gain a sense of power, and may feel invincible doing so since consequences are too far removed.

Broadly speaking, there may be a perception gap for children: These behaviors may be seen as a game in themselves or even a means to an end with little repercussions. For example, hacking and other issues have been used as tools for revenge–people took advantage of backdoor openings into systems because earlier problems were poorly managed, so they took it into their own hands.

These behaviors are further exacerbated by their normalization: *if everyone is doing it, then it is okay if I do, too*. Children are learning how to do some of these behaviors through social media, where they see others exhibiting these behaviors in an approachable way. Young viewers or members of social media groups become exposed to these behaviors from a young age and, through humor or casual discussion, come to learn that these behaviors are normal, acceptable, and can increase one's social status (i.e., "I can be like them").

Social media and social motivations are not the primary reason for youth criminal conduct or behavior and, again, we do not make claims to the causality or correlational relationship between them. The context of social interactions online and children's developmental milestones, however, must be considered as we continue to explore these behaviors.

Financial incentives

One of the other major motivations is financial, where the exploitation of in-game behaviors can increase one's real-world or in-game financial position. One example would be cheating in different game tournaments for cash prizes. At more amateur or semi-pro levels of gameplay, prize pools are large enough to attract hackers. As there may be multiple tournaments over the course of a week, cheating can be quite profitable.

There are other behaviors, however, such as hacking, that blur the lines of in-game and real-world harm. For example, hackers may hack a game for exclusive or rare in-game items and sell them to other players for real-world currency. In other instances, hijackers may take over player accounts and gain access to things tied to in-game value, like valuable skins or items, or real-world value, like credit-card information. Account takeovers then become a gateway for further types of abuse, such as credit-card fraud.

Intrinsic and in-game incentives

Finally, there may be some intrinsic and in-game incentives for conducting criminal behavior in games. One of these includes account leveling–hacking or using cheats to help level up one's character quickly. This may not be tied to external motivations like social clout or financial gain, but can be enough to drive one to such behavior. This can be extended to leveling up other players' accounts for profit, as well.

Another motivating factor is novelty and ease of access. As youth continue to develop their skills and push boundaries, it may become easier and easier for them to conduct criminal behavior. If they are bored, conducting such behavior may feel like a challenge as they test their new skill set.

What: Types, form and characteristics of behaviors

As the potential scope of this discussion is enormous, for the purpose of this convening we limited the areas of concern to the following: hacking (cheating and malware), intellectual property theft, hijacking (account and server takeovers), and information or server integrity (including doxxing, swatting, and DDoSing).

Hacking: Cheating and malware

Cheating and in-game hacking, such as the use of aimbots or wall hacks (e.g. Extra Sensory Perception), were one of the main behaviors discussed. One participant reported this problem to be a “cat and mouse game”, where identifying and addressing cheating was difficult. These cheats can be fairly complex and technical, and some people who develop them may even monetize them by selling them online for others to purchase and use.

A secondary layer to this cheating ecosystem includes malware. As people develop, share, and ultimately monetize their cheats or in-game hacks, some of this software may actually include malware. Unsuspecting players, including youth that may not know better, may download a cheat hoping to improve their in-game performance, and may unknowingly download malware instead. Malware is a larger problem for the mobile game space, but should be noted as it can also act as an avenue for account takeovers through methods such as cookie theft.

Intellectual property theft

One form of hacking that doesn’t directly harm players, but can be detrimental to game or game platform companies, includes intellectual property theft. This includes people who use hacking to gain early access to games that have not yet been released, or to discover unannounced details or secrets.

Hijacking: Account takeovers and server takeovers

Another major issue includes account takeovers: hijacking a user’s account, or hijacking player-defined servers by getting access to their credentials or authorization information.

With account takeovers, the hijackers are taking advantage of other players for their own gain, which often includes **financial gain**. With children or uninformed players, this may look like social engineering or simple requests for information (e.g., sharing passwords, sharing answers to security questions) that can be then used to access their accounts. This can and does at times escalate into accessing and reselling valuable in-game items, or stealing personally identifiable information and conducting credit-card fraud.

Hijacking on games with live server ecosystems may be particularly difficult to manage as these servers may not have a centralized team to help deal with the issue. There have also been reports of moderator accounts being hijacked for the power they may wield over a community or server. In some instances, this compromises the player base or servers through automatic bans, or attacks that are difficult to reverse engineer and may prevent servers from being restored quickly.

Additionally, there is sometimes a **social motivation** layer to these server hijackings. There have been instances where people hijack servers to build clout–they will brag about it and even stream their hijacking on social media. At times, these streams even receive donations from viewers, further normalizing this conduct.

Personal information integrity (doxxing), swatting, and DDoSing

Personal information integrity, or doxxing, includes when personally identifiable information, including names, financial information, or home addresses, are shared without the information subject's consent. In some instances, this leakage may be inadvertent such as when a streamer may not realize they are sharing their home or IP address live or when a child cannot reasonably consent (see youth vulnerability below). But in some cases, it can be malicious such as in cases where doxxing is paired with swatting. Swatting is understood as a high intent and high severity behavior as it can result in emotional and physical harm (up to and including accidental death).

Swatting is often reported as a tool of coercion or manipulation. For example, one form of swatting involves players receiving pizzas they didn't order as a form of threat, signaling that another person knows where they live. This can escalate into a form of blackmail, where the perceived threat is used to achieve a perpetrator's financial incentives, such as sending in-game currency or items to be sold for real-world currency.

DDoSing has been reported to be rare, but severe as it can render a server, game, or ISP inaccessible for extended periods of times. This makes it so players and game devs are unable to access their game servers. In some instances, these DDoSing attacks are caused by repeat offenders that do it for intrinsic reasons, such as sharpening and testing their skills. Some server-based games even see DDoSing attacks as a form of friendly competition between servers.

Incidence estimations and severity of harm

At the time of the workshop, the membership reported not having a good understanding of the prevalence of these issues. Participants did note that the extent of the issue is non-trivial, however. In particular, they called out that while some of the core behaviors do not happen often on their platforms or games, they are **highly severe** for their companies and for the players that are affected. See section on impact for more information.

As the industry moves towards measuring youth criminal conduct on their platforms or games, it may not be enough to understand prevalence. Metrics that track the severity of harm should be considered in tandem with prevalence to help determine the prioritization of work.

Understanding the impact and challenges

The following parts of the discussion explored the impacts of these criminal behaviors in gaming and challenges in addressing them.

Impact

The impacts discussed roughly fall into four categories, described below.

Perception Shifts

Exposure to criminal behavior or its aggrandizement can shift the perception of what is acceptable or even desirable within a community. By extension, young people are more likely to engage in criminal behavior as it becomes normalized, mistakenly interpreting such conduct as “not a big deal” or even that it is socially optimal in order to fit in.

In similar fashion, criminal behavior often escalates; a more severe infraction may seem less serious when it is perceived as just a small step up from another infraction. This leaves young people more likely to experiment dangerously as well as more vulnerable to bad actors who might take advantage of this priming.

Player Impact

While the intent behind some of these acts may feel innocent enough to young perpetrators, these behaviors can lead to a criminal record and as discussed above increase the likelihood of becoming involved in more serious crimes in the future. Thus, what might be seen as a “harmless” prank in the near term can have life-altering consequences long term.

Players who find themselves the victims of these criminal acts can be harmed in a myriad of ways, from the loss of their accounts or digital property, to violations of privacy, to trauma and rarely even accidental death as we’ve seen with swatting. More generally, exposure to such behavior has negative consequences for mental health and wellbeing, and can impact a young person’s overall capacity to thrive.

Trust and Reputation

The presence of criminal behavior in gaming spaces can damage player trust among each other and the reputation of the game maker or platform. If players feel unsafe they will be less comfortable engaging and may churn, while new players may forego a game altogether.

A reputation of poor behavior, such as cheating, can also lead to assumptions of that behavior even when it is not present, worsening perceptions of the product and community. This is exacerbated both by the fact that high-skill play to the average player can be indistinguishable from cheating and that playing poorly is often explained by the other person “surely having cheated”. One study from a participant’s company in 2018 showed that 15% of subscribing players churned from the game when they thought they had been exposed to cheating, underscoring this impact.

Business Repercussions

In addition to reputation and a loss of player trust, these acts can have direct and indirect financial repercussions for a company. Server outages not only lead to a direct loss of profits but further damage a company or game’s reputation, eroding the overall viability of products. Theft of IP can, among other things, interfere with a company’s ability to successfully launch titles, destabilize in-game economies, and potentially attract the wrath of players when ideas are prematurely exposed. Players may also abandon games when they perceive that other players may advance by cheating.

Criminal activities can also negatively affect employee health and morale, reducing their overall wellbeing. In some cases employees may even be targeted directly by these acts (e.g. doxxing).

Challenges / barriers

As the industry identifies avenues to mitigate these behaviors, we are faced with challenges and barriers that range from tactical execution on our platforms to addressing broader social systems. The section below summarizes those noted in the workshop, but may not be extensive.

Youth's Development and Vulnerability

Youth's susceptibility to conducting criminal behavior can be related to their developmental progression, including the way they learn and develop social norms. As children develop, they are learning about social norms and boundaries, with play being a critical factor in identifying what might be acceptable and what transgresses those norms. Young people at times view exploits in games and game systems as an opportunity to test their skills and, at younger developmental ages, do not recognize that there are real-world consequences to enacting criminal behavior.

When thinking about children's vulnerability to this type of harm, it is important to consider their **developmental age,** or how cognitively developed they are, over their physical age. Some children at the same physical age may have matured at a faster rate than others. Generally though, younger children may be more easily misled or are more trusting of those they interact with. This leads to increased risk when they interact with malicious actors using games to enact criminal behaviors, such as hijacking, swatting, or DDoSing. Children sometimes put trust in people they meet online and share personal information or passwords. One participant in the workshop mentioned an instance where a child was at home sick and mistakenly believed that the other player they were speaking to was also a child sick at home, when in fact they were not.

Teenagers and young adults may be more aware of the vulnerabilities and risk they incur, but take a more blasé approach: They know it's risky, but they don't care. The benefit of notoriety or social status–being seen as "cool"–or what they hope to accomplish outweighs the perceived risk of the criminal conduct itself. Additionally, teens and young adults may recognize the risks of being online, but may not understand the severity of harm associated with them. This may result in a casual approach to their account security and online interactions. One participant shared an example of their child signing up for a new account on a gaming platform, and their friend telling them to "just pick an easy password that's easy to remember." The participant reported having to intervene and educate on the risk of an "easy password".

Social Clout and Reinforcement Loops

Addressing the social contexts around criminal conduct in online gaming will be a core component to mitigating it. Performing criminal conduct on social media and receiving attention for it creates a reinforcement loop: As an individual gets more exposure for conducting criminal conduct, the more likely it is that this behavior is normalized. As people stream or share their criminal conduct online, they are likely to implicitly endorse these behaviors to their audience who then learn that these behaviors are benign and without consequence. Additionally, online social interactions' super power–the ability to develop and maintain a community with a set of shared interests–becomes detrimental when members of these communities make criminal behavior central to their online identity and sense of belonging. This can make it harder to change one's beliefs about criminal behavior, and to leave a community grounded around these actions.

Ease of Access and Cultural Norms

Another challenge includes the ease of access to the knowledge of how to conduct criminal behaviors online. At times, youth may engage in online communities that lend to the normalization of these behaviors, as mentioned above, and provide learning avenues in how to conduct them. Some youth may partake in these activities as an educational exercise where they want to improve their skills or improve their gameplay. However, in other areas of the world, these behaviors may be taught in more systematic ways as part of classroom curriculum. In some of these regions, the perception is that hacking or similar criminal conduct are interesting and valuable skill sets to have, and everyone should know how to do it.

No One Size Fits All for Caretaker Education

When it comes to developing security solutions for youth, one common response is to increase parental or caretaker education around the issue. However, there is variation in caretakers' access to technology or online games and security. Assuming a baseline level of caretaker knowledge will benefit those with access to these technologies, but could be detrimental to caretakers with a different set of needs and responsibilities. Some caretakers may not have the time or capacity to learn about the dangers of criminal conduct in order to discuss with their youth due to language barriers, workload, or other caregiving responsibilities. Information and educational materials need to be easily accessible, especially for caretakers who may not have the time to read through research reports or full articles.

Additionally, even if youth have a caretaker, they may not find them trustworthy or someone they can confide in or speak to about sensitive topics Furthermore, video games are often trivialized or stigmatized, so it may be an uncomfortable subject to broach. As the industry moves forward with identifying educational pathways for caretakers to speak to their youth, we must consider the diversity of needs and ensure we develop resources for everyone.

Lastly, even a technology-savvy caretaker may struggle to know how to navigate what is an incredibly complex ecosystem. Parental-control systems, for instance, are often different for every game, and as one person in the session lamented, are often poorly understood by even the developers themselves. Thus, it is asking a lot that a caregiver be fluent in all such systems their child may encounter. Greater consistency and standards would help alleviate some of this burden.

Improving Law Enforcement Processes and Cooperation

When companies are faced with criminal conduct on their games or platforms, it has been difficult for them to know how to work with or reach law enforcement. Some companies expressed that it is unclear who they should contact and what type of information they need to provide in order to help any investigation.

Overall, there is interest in potential partnerships with law enforcement and the Department of Justice that result in the co-development of a guidebook or framework on how to coordinate with them. Developing these potential resources, however, could require producing guidance concerning state, local, and federal law enforcement. On top of that, many games have an international reach, which further complicates the content of any guidance and the law enforcement reporting and cooperation. For example, if a company is based out of the United States of America but the criminal conduct stems from another nation, who has jurisdiction and what might those partnerships look like?

Tactical Challenges for Game Devs and Platforms

On top of the broader systemic challenges named above, games and gaming platforms face tactical barriers to addressing criminal conduct, as well. At times, addressing criminal conduct can feel like a “cat and mouse game” where companies can address one issue only to have more arise. This is indicative of how difficult it is when there are no systemic measures in place to proactively address these issues. As such, solutions can feel reactionary and inconsistent, including common safety systems like reporting functionality. While reporting tools can be useful after the criminal conduct has occurred, they are at times insufficient: They’re often not adequately used, not understood well by users, poorly designed, or an insufficient tool in the cat-and-mouse game.

Internally, gaming companies can face difficulties when there is inconsistency around expectations. Differences in enforcement can cause this, such as when there are multiple people or departments who work with various subsets of a game’s audience (e.g. between regional offices or those who work with pro or semi-pro players vs. amateur players). Inconsistency can also be exacerbated by business directives that may be biased when a problematic player is also considered a reliable source of income, such as the case with popular streamers. These apparent double standards can create tension throughout a company and can undermine other efforts to dissuade criminal conduct as players see different behavior modeled.

Generally, decentralized services and distributed systems create further challenges in the system if they cross regional barriers with different regulations. It can be difficult to know “where” the crime occurred or who has jurisdiction or responsibility over what has transpired (or may transpire in the case of more proactive measures).

Companies with global player bases may therefore struggle to stay apprised of the many nuances of the various regions in which they operate, while these differences may lead to very different player interpretations of what is acceptable. As an example, account sharing, which may be a violation of a company’s Terms of Service, is encouraged in some cultures who highly prioritize sharing between siblings or close friends. Such attitudinal differences may result in weaker security around accounts, or differences in perception of the inviolability of accounts more generally.

Other observations/insights

Participants in the workshop reported variations on what they considered to be their top problems. For some it was cheating and hijacking while others were focused on DDoSing and swatting. These variations may be an outcome of their game or game platform system design that provide different incentives and affordances. Server-based games reported being targeted by DDoS attacks, for example, while first-person shooters may be more prone to cheating and hacking. Beyond that, each company may have different prioritization for top concerns and where to put their resourcing.

With the Covid-19 pandemic came an increase in DDoS attacks and other types of criminal conduct. Some game platforms reported an increase in attempts to take their game servers down. They hypothesize that with increased time at home, children who were bored spent the time learning these new skills and were testing them.

Finally, efforts toward Web 3.0 and related metaversal technologies are adding ever greater decentralization and anonymization to the mix, which are exacerbating existing challenges for developers and regulators as well as introducing new ones (such as the impact of digital assault in high fidelity environments). As the technology improves to allow for persistent and nearly unlimited server sizes, modern online spaces are outpacing our ability for effective oversight. Questions of accountability and culpability are increasingly more blurry for both developers and players.

Meanwhile, the growing popularity of alternative digital currencies is itself a new frontier that is commoditizing technology in new ways. The result is a preponderance of temptation for young people bolstered by the “anything goes” atmosphere of these new digital playspaces.

Addressing youth criminal conduct in gaming

What we're doing/thinking about

Establishing Norms: Youth-Focused Education

Since one major motivational incentive is social clout, with these behaviors being normalized online one of the most salient opportunities is to develop youth-focused education to help model good behavioral norms. This may include partnerships with popular influencers to model good behavior in games or on platforms. This could be part of a larger digital citizenship initiative, where youth are taught how to engage responsibly with others online through empathy and respect. This focus on digital citizenship could also broaden our current understanding of traditional citizenship to the online world, where civic support structures like law enforcement or community care models are found to support norm development and creation as well.

Games and game platforms can integrate youth-focused education onto their surfaces to increase exposure and normalization of prosocial norms and behaviors. This may include age-appropriate and relatable tips that are baked into onboarding on what a positive game culture looks like, or warnings against criminal conduct or disruptive behavior. The exact placement and timing of these tips or warnings for peak efficacy is an open question, but some companies have already been experimenting with these methods with some early success.

On top of increasing education to drive prosocial norms, there is also the opportunity to make account security more accessible to youth through educational programs or on-platform efforts. Youth may be aware that they need to create strong passwords, but explaining *why*–that there are people who may try to access your account and take your things –and *how*–people may ask you questions to get your account information or security questions–we can work towards creating a more resilient community of young game players.

Increasing Access to Information

As discussed above, some caretakers may have lower tech literacy or may not have accessible information to help open up conversation on these topics with their children. Additionally, in some regions like India, it is more common for people to share information in alternate forms such as jpegs on social media like WhatsApp. As the industry moves towards educational pieces for caretakers, and even for youth themselves, we should consider developing highly accessible and absorbable information, including shareable images with everyday language to make the topics easily understood.

Game design and technical solutions

As game developers, we have an immense opportunity to shape the culture in our different communities. One possibility includes providing in-game rewards for behaviors, which promotes a culture of positive play and discourages criminal or disruptive behaviors. By uplifting behaviors that promote prosocial cultures, we develop positive reinforcement loops. At the same time, creating clear, consistent consequences to criminal behavior—and communicating them in a transparent and timely manner—helps break the reinforcement loop that normalizes such behavior.

Games and game platforms also have the opportunity to expand their enforcement strategies when criminal conduct occurs. Zero-tolerance policies, such as banning transgressive players from games or disabling accounts, might be effective. One complication, however, is that users can potentially create secondary or spoof accounts to counteract these methods. Additionally, hardware banning may be effective, but may be infeasible for locations with shared networks such as internet cafes or universities.

Finally, to help with variations on account security, games and platforms could require multi-factor authentication and beyond to help bolster their player community's resilience to hijacking attempts. This may include exploration into other forms of identity verification, such as uploading a government ID or sharing more detailed personal information, to help the platform confirm one's identity.

Where we need to go

Short-term (i.e. next steps from this workshop)

We face a myriad of challenges in effectively mitigating youth criminal conduct in gaming. This initial conversation was intended to first explore this space and those challenges, and to gauge an appetite for future efforts. It is clear from our convening that there seems to be a general consensus on the importance of this work and an eagerness to tackle these challenges together as an industry.

The following are some recommendations for next steps in the near term:

- Convening a series of more targeted, action-oriented discussions on key aspects of the problem space with the aim to establish a working group with specific outcomes and deliverables as appropriate. Topics to consider that were raised during our meeting:
    - Barriers to contacting and working with law enforcement and best practices
    - Understanding and assessing the prevalence and severity of the issues discussed here.
    - Design frameworks for proactively reducing this conduct. (Where are the high value interventions in the possibility space? What is in the way of enacting these or creating the space to explore these interventions?)
    - Best practices for penalties. We can't proactively address everything, but how might we improve awareness and self-reflection through our penalty systems?
    - Education. How might we enhance education more generally on these topics? Could game companies potentially partner with schools, influencers, or other avenues of high connection with youth?

  - Parental controls and support. It is clear we've a long way to go here, so what are the next steps and how do we unblock them? How do we work more effectively with platforms?
  - Platform-developer relationships. How can platforms do more to support not just players and caregivers but developers?
  - Differences among the scale of developers (indie through to triple A). Going deeper on the differences between large and small developers, developers and platforms, and other key differences.
  - The complexity of these issues on a global scale, with an eye to regional differences.
- Creating a broader invitation to share best practices on these issues.

Long-term as an industry

Longer term, there is clearly a need for some better resources and practices to help developers address these issues more effectively. As well, the nature of the challenges with criminal conduct mean that we are never going to fully eradicate these issues, so there is an evergreen aspect of this work to keep in mind. With that in mind, there are some recommendations for how we continue to progress this work.

- An intentional effort to synthesize and make available best practices for the industry to help existing developers, as well as help smaller or new developers who may be less equipped to handle these kinds of challenges.
- Exploring workshops and other educational formats in partnership with other organizations. For example, how might we help both developers understand how best to work with law enforcement and equally help law enforcement better understand gaming spaces.
- Follow-up conversations, like this one, to check in with how we are doing as an industry and with the support of organizations like the DoJ to help inform the scale of the problem and the latest understanding from experts in criminal conduct.

We invite FPA members, other game companies, or related organizations with an interest in being involved with these efforts to reach out to the Fair Play Alliance, as well as to share additional ideas or existing work.

Glossary of Terms

- **Account takeover:** Accessing another individual's online account without his or her authorization and using it to commit fraud or other unlawful acts.

- **Chatham House Rules:** Rules governing a meeting where participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

- **Criminal behavior**: According to the U.S. Sentencing Commission: "Traditionally, youthful offenders often have been defined as those under the age of 18, but for purposes of this study, the Commission has defined youthful offenders as federal offenders 25 years old or younger at the time of sentencing. The inclusion of young adults in the definition of youthful offenders is informed by recent case law and neuroscience research in which there is a growing recognition that people may not gain full reasoning skills and abilities until they reach age 25 on average."

- **DDoS or Distributed Denial-of-Service Attacks.** A form of cyberattack in which the perpetrator disrupts a network by overwhelming its infrastructure with traffic, typically through compromised computers who act as the source of the traffic.

- **Doxing:** Publishing private and/or personal information on the internet about an identified individual or organization, typically with malicious intent.

- **Hacking:** Repurposing a code, system, or code to perform in a manner unintended by its creator. Hacking may be conducted lawfully or unlawfully.

- **Intellectual Property:** Intellectual property consists of creative works protected by copyright, brand identification protected by trademark, and novel inventions protected by patents and trade secret law.

- **Swatting:** Making a false report of a violent threat to emergency services so that a law enforcement response is dispatched to a target's address.

- **Threat:** Under federal law, an interstate or foreign communication containing a threat to kidnap or injure another person is a violation of law, if it is a sincere expression of the intent to commit unlawful violence.

FAIR PLAY ALLIANCE

For additional information or for further resources, please visit https://fairplayalliance.org/