GUIDE TO PLATFORM SAFETY, SECURITY, AND PRIVACY

by Hemanshu (Hemu) Nigam
Last updated: March 2019

Introduction

It is possible for online platforms to create a clean online environment, and it takes work and effort, but it is worth it. Any online platform that is truly committed to making the Internet a safer, more private, and more secure environment must take proactive steps to implement safety, security, and privacy into its culture. Platforms can implement a host of technology, policy, and programmatic solutions that enhance user privacy, reduce the threats of unauthorized personal data disclosure, prevent attacks on consumers, mitigate the amount of unlawful or unwanted content, and deter illegal behavior.

As a safety, security, and privacy expert who has been in the front lines of preventing or prosecuting abuse on online platforms for over 21 years, I can confidently say that the industry has the means, the know-how, and the resources to accomplish these goals. Yet, action is needed.

Recent events have shown that platforms have failed to prevent dangers that arise when they turn a blind eye towards obvious and preventable harm. This was known in advance of Cambridge Analytica and other recent damning revelations. In fact, the Digital Citizens Alliance authored a series of reports revealing serious and disturbing issues that were the direct result of platforms making conscious and deliberate decisions adversely impacting piracy, human trafficking, spying, privacy, illegal drugs, financial crimes, trojans, ransomware, and more. DCA's investigative reports can be found here.

It is quite clear that platforms are essential facilities in our online lives. Thus, these platforms must take on roles like those of any responsible community leader. They must create clean, well-lit neighborhoods for their customers and citizens. They must educate, provide protection, set strong policies, and deter and punish bad actors. These might be private businesses, but they come with a simple requirement – run your operation much like the communities we all physically live in. In other words, care about those who are in your online communities and be responsible for protecting their safety, security, and privacy.

Who Should Use this Guide

This guide is a must for any company which provides an online platform for user generated content, where users connect with, create, consume, and share such content with others. It is a simple set of prescriptive actions that will increase safety, security and privacy online. All of these have been done by major sites, and all of these can be done by today's online platforms that fall within the purview of this guide. This guide is a must for any platform that is designed for the purpose of inspiring user generated content or provides users the ability to access user generated third-party content. It's that simple

Platforms must recognize that success comes from developing a close, cooperative working relationship with governments, policymakers, law enforcers, and NGOs. This coupled with a foundation of safety, security, and privacy that includes consistent and persistent technology development, user education, NGO partnerships, law enforcement support, public policy initiatives, and industry cooperation can and will lead to success when protecting the fundamental rights to safety, security, and privacy of the users who access these platforms – adults and children alike.

General Approach to Acting Responsibly

As a starting point, platforms should focus on the four "C's" of properly protecting users on their sites:

- Content – prevent access to inappropriate content
- Contact – prevent unwanted contact between users
- Conduct – prevent unauthorized disclosure of personal data
- Collaboration – partner with law enforcement, advocates, law makers, and educators to enhance safety, security, and privacy as a community and raise awareness in these areas

Online platforms have historically taken a reactive approach. Those days need to end. It is now time to provide a combined reactive and proactive approach to safety, security, and privacy, as others have done successfully.

Responding to issues only when someone else raises them is a recipe for failure and a purposeful abandonment of responsibility. Time and time again this has proven true, and the recent "Zuckerberg Hearings" are perfect examples of that.

A central component of approaching platform responsibility is to adopt solutions that society has implemented in the physical world into the online world. More specifically, platforms can take a proactive, comprehensive, and holistic approach that involves the following elements working together:

- Site-specific safety features, policies, and practices to address illegal and otherwise harmful content
- Cooperation with law enforcement and collaboration to the extent permitted by law
- Engaged and informed parents with access to tools to protect their children

- Easy to use tools for members to protect themselves, to defend their privacy, and to report abusive contact or content
- Robust safety educational information available to members, parents, and teachers
- Clearly articulated reasons when personal information will be disclosed or shared and, methods for reducing unauthorized access or disclosure
- Collaboration with organizations that promote online safety, security, privacy and customer education

In the end, platforms have an opportunity to send a clear and focused message to wrongdoers and criminals: We do not condone unlawful or illegal conduct and have implemented a holistic set of policies, tools, people, and partnerships to prevent harm online.

And the best way to send such a message is to implement the following policies, programs and tools.

Note that none of this matters unless platforms are actively taking on the challenges they face, rather than simply relying on their users or technology alone.

SAFETY FEATURES

- **Image and Video Review:** review images and videos that are uploaded by users including those that are linked to third party servers for violations of policy such as extreme violence, pornography, drugs, hate speech, child exploitation, or beheadings.
    - **Note**: Often platforms state that too many hours of video are uploaded making the task of video review impossible. That is false. With little engineering, platforms can create randomly selected still images from a video to review and flag for further action. Video and images can also be prioritized by using artificial intelligence tools that many companies already use for business purposes.
    - **Note**: Often platforms state that content can return via other sites. Solutions for this issue are widely available and easy to implement. For example, a "fingerprint" of an image or video file that has been identified as violating policy can be placed on a content blocking server. This server can easily be checked each time new content is uploaded to block the bad image of video. In addition, the URL of where the content resides can also be fingerprinted and scrubbed from the platform.
    - **Note**: similar solutions can be implemented for links to known illegal or unlawful sites with little engineering and no impact on user experience.

- **Enforcing Age Limits:** platforms almost uniformly set a minimum age at 13 years old to avoid the stricter requirements of COPPA. While there is currently no effective age verification mechanism due to technical, legal, and data challenges, platforms can still deploy a variety of technical solutions and procedures to enforce the age restrictions. The FTC has set clear expectations in this area, and various implementations can be done without hurting the user experience.

  - **Note:** Sites often suggest that users can get around age restrictions by changing their date of birth. Sites can utilize session cookies and other technical measures to prevent abuse. Sites can also provide easier reporting mechanisms so underage users are easily flagged for review and deletion.
  - **Note:** Sites often state that users can return easily. True, but simple technology has been used to identify underage users via their connections and other means.
  - **Note:** Sites state that users can get around these age restrictions if they are already aware of them. Sites can deploy search algorithms that identify commonly used underage terms and update such algorithms to review and remove proactively any identified accounts. These algorithms can run 24/7 flagging accounts for support teams to review and investigate.

- **Privacy Settings:** Platforms need to strengthen their default privacy settings. Many have settings that make clear decisions on the type of personal information that will be disclosed to others. Platforms need to thoroughly re-evaluate what those default settings are so consumers are better protected from abuse and unauthorized disclosures. In addition, privacy controls need to explain in simple language what data is collected, how is it used, who it is shared with, and when is it disclosed. Fundamentally, user data is called that for a reason – it is user data. As such, the user should be given full knowledge of what is happening with their personal data at all relevant times.
  - **Note**: Platforms often state they do in fact inform users about their privacy rights and tools available to them, but users are still surprised to see personal information shared or disclosed. While it is easy to blame the user, it is much like blaming all the students when a teacher doesn't teach properly. Users are often surprised by what happens because they were not educated and informed in terms they would understand.
  - **Note**: Platforms can also solve these challenges by utilizing teachable privacy moments – informing users what is about to happen with their personal data at the moment the train is set in motion.
  - **Note**: Platforms often act surprised and use well-worn apologies when their users discover that their personal data was shared in ways they did not approve. It is critical that platforms use traditional methods of educating users at the moment a privacy related event occurs. This is often called a teachable moment, and users have been shown to respond positively to these.

- **Users Empowered to Report:** Platforms persistently rely on users to report content or conduct that violates the law or their terms. While such notice and take down policies are effective when used, they must be secondary to proactive efforts to identify, remove, and block harmful conduct and content. Nevertheless, platforms often make it a challenge to report abuses. The ability to report abuse must be present wherever user generated content exists and must be intuitive.
  - **Note:** Platforms should implement reporting tools that are intuitive and easy to find. On the back end, reports should grab at least the URL of the content being reported along with the reporting person's account information. Abuse teams can then look at what is being reported without the need for extensive investigations.
  - **Note:** Platforms will often simply delete content that is reported without looking at other issues that might be prevalent. For example, a person may be reported for unwanted contact with another. Abuse teams should look at other types of conduct the abuser may have engaged in to identify other issues that might require a report to law enforcement.
  - **Note:** Platforms often provide confusing and counter-intuitive mechanisms for reporting abuse that are clearly designed to disincentivize users from reporting issues. Users are often presented with choices that either make no sense or are confusing, disincentivizing users from making legitimate reports of abuse. For example, one platform requires a user to choose 'I think it shouldn't be on 'SocialMediaSite'' when trying to report a post that advocates gun violence. After two additional counter-intuitive steps, the user eventually locates the correct reason for the report. Finally, reporting features are often hidden under 'Options', a choice that has no apparent connection to where one might be expected to report abuse. Platforms can easily choose abuse mechanisms that are intuitive and mirror user expectations, without impacting user experience.
  - **Note:** Platforms often rely on users to search the Help section for ways to report certain conduct or content. This extra step can cause permanent harm due to the delays it creates or the disincentive to report. Specifically, sites can include a link to "Report Abuse" at the bottom of every page that contains user generated content. Additionally, links to report abuse can be provided in other areas containing user-generated content, including direct messages, videos, photos, and comment postings.

- **Teachable Moments:** Platforms must utilize teachable moments for users on why certain security or privacy mechanisms are in place so that users are constantly educated and learn to become better online navigators. For example, platforms can educate a user when they are clicking on a link that might be malicious or when they are searching for content that may be illegal or unauthorized.

    - **Note**: Platforms often think teachable moments interfere with the flow of their site and user experience. Quite the opposite is true. We live in a world filled with teachable moments. For example, road signs that warn a driver of an upcoming curve, flashing lights that warn a driver going too fast. Signs inside a grocery store when the floor is wet. Sites can create the online version of these often called interstitials. When a user is about to make the wrong turn on a site, platforms can place an educational warning.
    - **Note**: Platforms often complain that they don't know if a link might be harmful. The facts on this are clear. Numerous security researchers have created databases of known bad or illegal sites that platforms can tap into and integrate into their own systems. In fact, nothing in the law prevents platforms from collaborating with other platforms and experts to share such data and then block harmful sites.

- **Remove Registered Sex Offenders:** Platforms that allow communication by adult users with children users should block registered sex offenders. This is done simply by requiring registration data that can be run against the registered sex offender databases. This then prevents access by sex offenders or limits their ability to connect with minors, at the very least.
    - **Note:** Platforms might argue that such measures are against offender rights. However, more than 40 states already require registered sex offenders to register their email addresses with the states. In fact, a federal law exists here as well. Sites should check against these databases to ensure compliance with the law and to take further action.
    - **Open Disclosure:** The author of this guide's company, SSP Blue, offers registered sex offender prevention solutions to platforms.

- **Crisis Intervention:** Platforms should create mechanisms for users to quickly and easily seek help in a crisis or to report a potential crisis. With online environments being a haven for troubled adults and teens to post their cries for help, platforms have a responsibility to put in systems that bring such issues to the front of the line for action by law enforcement and other experts.
    - **Note:** Platforms consistently claim that they were not aware of an impending issue even though the user was clearly posting a threat or cry for help. Platforms can use drop down menus that allow for easy on the spot reporting by other users. For example, a suicidal posting should be easy to report followed with a specially trained team that knows how to get a wellness check done in less than 30 minutes.
    - **Note:** Platforms often state they partner with mental health experts. Unless mechanisms exist to trigger their involvement when critical, then such partnerships are often just PR moves. Platforms can proactively reach out to local law

enforcement if they are proactively reviewing content. This can prevent school shootings, teen suicides, and other tragic incidents.

- **Email Verification:** Platforms utilize multiple sign up methods in order to quickly grab a new user. Email verification systems remain a useful method of reducing anonymity, thus deterring bad actors from creating new accounts. In addition, such verification reduces spam and helps law enforcement track down criminals.
  - **Note:** Platforms are often simply asking for an email and password without any confirmation whatsoever. This allows bad actors to create multiple accounts using bots. It also let's wrongdoers create accounts to engage in unlawful or illegal activity and remain unreachable from the hands of justice.
  - **Note:** Platforms often state that email verification processes are not reliable. And yet, every single online person today has an email address. If they are unreliable, it is because the platform is dealing with a wrongdoer who doesn't want to be identified. Therein lies the core of the problem.

- **Safety Center:** Platforms should create a resource center specifically focused on safety – what is expected of users and how to handle issues that may arise during their use of the site. Such a center should be easily accessible and easy to navigate, and mobile friendly. Given the number of non-users who may need assistance from a platform support team, such a center should also have a dedicated area for non-users to seek information and help.
  - **Note:** Platforms must include sections for users, parents, and law enforcement outlining everything from what their policies are to who to contact when a person tries to report an issue.
  - **Note:** Platforms often hesitate to provide information or reporting ability to anyone who is not a member of their site. This creates situations where a parent can't get help for their user child or for law enforcement who can't quickly identify who to get in touch with in case of an urgent matter or routine investigation. In the physical world, no such concept exists. A person walking down the street has no difficulty in reporting an incident they see occurring on private property.

- **Dedicated Team for Customer Care:** Given the prevalence of highly sensitive issues that platform support teams face, it is critical to implement dedicated, specialized teams to handle sensitive issues 24/7/365 such as cyberbullying, impostor profiles, harassment, and terrorist recruitment. Timely reviews and action can make the difference between a user staying safe or being in critical danger.
  - **Note**: Platforms often state they already have large support teams ready to handle user reports. Repeatedly we see reports get no response from platforms or unduly delayed responses. Dedicated teams for sensitive matters can receive sensitive

reports at the top of their queues, making the difference between life and death. These teams can also conduct deep searches looking for related issues and identifying organized groups of wrongdoers.

- **Preventing Minors from Accessing Age-Inappropriate Content:** Platforms must prevent content on their site that is inappropriate for minors on their sites. If platforms want to allow content that is for adults only, they can always turn their sites into 18+ communities. If not, it remains their responsibility to prevent content that is not suitable for minors.
    - **Note:** Platforms often state that they will remove content that violates their terms once they are notified. This notice and take down policy does not prevent a minor from seeing the content. Platforms can proactively monitor their platforms so that minors never see the content in the first place. This can be done through a variety of measures from fingerprinting and preventing uploads of known bad content to using artificial intelligence to flag and prioritize content for moderator reviews. While these methods are presented simply, the reality remains that such capabilities have existed for over 15 years.

- **Group Review:** Platforms can prevent the creation of groups that are secret to the point that even the platform doesn't know what is in them.
    - **Note:** Platforms claim that such secret groups allow for the free flow of ideas especially in suppressed regimes. If we allowed secret stores where the mall owners didn't know what was happening in them and no way of finding out, we would ban such stores in an instant. The same is true here. The moment real anonymity is created, these groups become a haven for criminal and unlawful activity.
    - **Note:** Platforms should endeavor to balance free speech with the ability to identify criminal conduct by setting up triggers for review. While privacy is important, it cannot be used as a shield for allowing criminal activity that causes harm to other users or members of the public.

- **Partnership with NCMEC:** Platforms must do more than just report illegal child exploitative content that is reported to them. The National Center for Missing and Exploitation Children has the know how and programs designed to proactively identify, report, and prevent child exploitation on platforms.
    - **Note:** Platforms can showcase their efforts by reporting as required by law and by using photo DNA technology. These are just basic, minimum steps, that platforms should take. Proactively, platforms can automatically fingerprint any video or image that contains child exploitation and use that to scrub their systems. Whether search or social, these principles are easy to implement with no new technological developments.

SECURITY FEATURES

- **Interstitial Pages:** Platforms can continuously warn users when they are leaving their site or clicking on something that is unknown to prevent users from ending up on phishing and malware sites.
    - **Note**: Platforms often state that users can freely create a link out to a dangerous site and they wouldn't know. The fact is numerous organizations have created databases of accessible known bad sites that can and ought to be blocked from access by these platforms. Once identified, these links can be prevented from being posted and scrubbed.

- **CAPTCHAs:** All platforms should utilize CAPTCHAs, which are simple visual gateway puzzles designed to be solved easily by human users but difficult or impossible for computers to solve in an automated environment. By requiring CAPTCHA solutions to perform specific activities on a digital platform, and by allowing users to have the option to require CAPTCHA solutions for certain methods of contact, platforms can drastically reduce spam and other unwanted contact on their services.
    - **Note:** Platforms believe that captcha's stand in the way of user experience, and offer no other reasons for not using them in various places on their sites.

- **Phishlocking Tool:** Platforms should stop spammers in their tracks by instituting "phishlocks" on user accounts that may have been compromised by a hacker. Spammers thrive on the inherent trust of communication users receive from friends to propagate their false advertisements and other nefarious conduct. Platforms can easily institute tools that detect if a user account may have been phished and "lock" it to prevent the account from perpetuating the advertisement until the user can update their password and solve a CAPTCHA. This is a great method for stopping the spread of fake news often perpetuated by bots and fake accounts.

- **Link Control:** Platforms can utilize a variety of methods to control the links that are placed on their sites by converting them in a way that the platform becomes the gatekeeper to a user's access to that link. As such, third party links can be immediately blocked if the platform identifies the link as malicious, spam, illegal, fake news, or anything else prohibited. This allows platforms to sweep clean their site with the push of a button.

- **Pattern Analysis:** Platforms can utilize pattern identifiers to look for anomalous behavior ranging from users who garner too many followers too quickly, have multiple accounts connected to a static IP, are utilizing VPNs and disseminating large amounts of information, are posting new content too quickly, are paying through foreign accounts for accounts that seem to be created locally, and the like. Users develop a pattern profile and unusual profiles should be immediately reviewed and action taken. This can easily identify fake news posters, spammers, and hackers.

- **Blocking, Filtering, and De-Listing Tools:** Platforms can use a variety of tools to block, filter out, and de-list known content that violates the rights of others or is illegal. Many rights owners provide constantly updated lists of such content, as do organizations protecting rights of victims which can be seamlessly integrated into blocking, filtering, and de-listing tools. This knowledge base can also be integrated into evolving algorithms that platforms can run proactively instead of engaging only in notice and take down practices. These algorithms can also work directly with recommendations engines to stop recommending content to users that violates the law whether it is a website, a video, or an image.

- **Comprehensive Spam Settings:** Platforms have shown their ability to implement successful programs and tools to prevent spam on their sites. A great deal of these efforts utilize solutions that can be implemented in responding to other challenges outlined in this guide. Platforms have used solutions like fingerprinting spam content to wiping and blocking it from their site, IP blocking, and sharing spam related data with others in the industry. These types of solutions can be used in other areas as well, such as identifying fake news and pirated content.

- **Users Empowered to Report:** Platforms must provide easy to report tools when it comes to users reporting spam, phishing, or other security concerns. Once reported, these reports must be reviewed by teams who can not only act on that report, but also take action site wide to minimize the spread of a particular problem.

- **Application Security:** Despite the proliferation of apps integrating with digital platforms, requirements of what data is shared, how it is used, and what apps are allowed remains a decision wholly controlled by platforms. As such, platforms must put user privacy and security at the top of their priority lists.
    - **Note**: Platforms often state they aren’t responsible for apps that might be nefarious in nature. Platforms can easily review every app that enters their platform using existing mechanisms and block apps that soak user data without authorization, spread malware, disseminate fake news, provide easy access to pirated content, and the like.

- **Hosts and Registrars:** Platforms must collaborate with hosting sites and registrars to ensure that issues involving spam, phishing, and malware are promptly resolved. While platforms can take down or block content from reaching their users, attacking the source prevents repeated violations or attempts.

- **Affiliate Networks and Advertisers:** Platforms must strengthen their review of who advertises on their networks given the ease with which advertisers can lead users to fake news and illegal sites.
    - **Note**: Platforms all claim to have guidelines that govern the type of advertisements they accept on their sites. This does little to curb advertisements that promote fake news sites, spread unsubstantiated propaganda, or lead consumers to phishing, malware, and pirate sites. Platforms can use existing technology to scrub ads before they go live and trigger human review for any anomalous behavior.
    - **Note**: Platforms can easily compare disparate data that shows signs of unlawful advertising. For example, an ad that has a link to a known phishing site, or takes payment from one region, but sells goods and services in another region shows a clear sign of unlawful conduct that ought to be reviewed by platform security teams.

- **Impacting the Internet:** Platforms have a unique opportunity to broadly impact the global digital environment if they choose to collaborate with other platforms. Just like in the physical world where policy makers, NGOs, and advocates share intelligence and information, platforms can share critical solutions and knowledge of unlawful conduct to help stop these issues on multiple fronts.

- **Government and NGOs:** platforms should employ experts who consult with government and NGOs with subject matter expertise.

PRIVACY FEATURES

- **Email Notifications:** Platforms must give users the right to choose what actions related to their accounts they are notified about to reduce the risk of phishers sending fake notifications. Default settings should be the opposite of what they are today and be changed to give less continuous notifications of activity on the site. While these notices are designed to promote platform usage, they are consistently abused by phishers and hackers who create similar looking notices to steal user data.

- **Privacy Settings:** Platforms must build intuitive privacy settings where default settings are easy to understand and easy to change. Users must have the ability to restrict access to certain personal information from sharing, disclosure, and usage.
    - **Note:** Platforms often state they already provide robust privacy settings and features. Yet, there is repeated user outcry when data is shared without authorization, or users are manipulated into thinking they have control via legalese in privacy policies. Users should never be surprised and this can be

solved by informing users of what is shared, disclosed, collected, and used in simple, easy to understand language.

- **Privacy Centers:** Platforms should create privacy centers that have simple explanations with videos and screenshots for users to get straight answers to privacy questions.

- **In the Moment Privacy:** Platforms must include privacy notices in the moment when setting up new accounts and when a user takes action to change existing settings, or when a user is about to disclose personal information.

- **Privacy that Mirrors Real Life:** Platforms can and should create privacy environments that mirror real life scenarios. Everyone has various circles of friends and contacts with whom they share certain things they don't share with others. Platforms can mirror these environments by providing users the tools they need to create similar online communities based around circles.

- **Application Privacy:** Before a user installs a third-party application, platforms must inform what information will be shared and the ways that application is allowed to use that information. While many platforms show what might be shared with an application, none show how the application may use that information. This fundamental shift will create immediate accountability for applications intent on misusing personal information and will help users make informed decisions on which apps to use.

LAW ENFORCEMENT

- **Criminal Prosecutions:** Platforms must proactively work with law enforcement in referring conduct that appears to be criminal. Just as police officers patrol neighborhoods across America and the world, platforms can patrol the neighborhoods they have created.
    - **Note:** Platforms like to showcase that they work with law enforcement when they respond to appropriate legal process. Platforms can proactively report issues such as predatory behavior, terrorist activity, identity thieves, hacking and malware attempts, illegal sales of drugs, and more. Nothing prevents a platform from reporting a crime, much like in the physical world where anyone can report a crime.
    - **Note:** Many platforms make it difficult for law enforcement to reach them 24/7/365 even though dangerous crimes and threats of immediate harm can happen anytime, anyplace. Platforms should provide the law enforcement community with easy to use law enforcement guides that lay out what data a platform has, how long it is retained, how to obtain it, and what their notification policies are.

  - **Note:** Platforms rely heavily on notice and report as opposed to proactively working with law enforcement. As stated above, platforms can help law enforcement reduce crime in society by working directly with them. For example, platforms can train law enforcement on how to use their platforms to investigate crimes or bring together multi-jurisdictional task forces to reduce the threat of certain crimes.
  - **Note:** Platforms often create an email address for law enforcement and stop there. Unless these emails are being monitored 24/7/365, platforms need a telephone hotline for law enforcement – this is the only way to prevent impending threats of harm or death.
  - **Note:** Platforms may be reluctant to share information with law enforcement, but nothing stops them from learning from law enforcement. In fact, platforms can learn a great deal of intel from law enforcement that can be useful to prevent crimes on their sites.

LEGISLATIVE STRATEGY

- **(Re)-Evaluating CDA Immunity:** The recent enactment of SESTA (Stop Enabling Sex Traffickers Act) allows for the prosecution of interactive service providers who often avoided any liability by claiming immunity under Section 230 of the Communications Decency Act. (See: https://www.congress.gov/bill/115th-congress/house-bill/1865/text and http://thehill.com/blogs/congress-blog/judicial/388694-sesta-fosta-imposes-accountability-on-internet-service-providers). Such a law showcases that the CDA cannot be used for blanket immunity and must be evaluated in the current climate where platforms have used it as a way to avoid any type of responsibility whatsoever.
  - **Note**: Recently a Georgia Court of Appeals laid out factors to consider when evaluating whether an interactive service provider can face liability. (See: https://images.law.com/contrib/content/uploads/documents/404/14125/Ga.-COA-Maynard-v.-Snapchat-June-2018.pdf). Policymakers, prosecutors, and civil litigants should not assume that CDA immunity applies simply because platforms are considered interactive service providers who are merely publishing third-party content. This is not always true and must not be assumed to be de facto. Rather, an evaluation must be done to see what role a platform had vis-à-vis the alleged unlawful or tortious conduct.

PREVENTING ACCESS TO PIRATED CONTENT

- Platforms must build more robust mechanisms to stop piracy. Many pirate sites rely on platforms to deliver customers and victims through unlawful advertisements, spam campaigns, and search engine optimization efforts.

    - **Note**: Platforms often claim that they cannot be held responsible for knowing what is pirated and what is not. Content rights holders and law enforcers continuously work to identify such pirate content and sites, but accessing them remains easy without the proactive cooperation of platforms. Notice and takedown has failed to stop piracy and counterfeiting. Formally identifying pirated sites, especially those found abroad, and placing them on black lists will prevent access to them from platforms. In theory, this is no different than what platforms already do when blocking known bad IP addresses, spammers, or child pornography.

EDUCATION AND OUTREACH

- Collaboration amongst law enforcement, schools, community groups, policymakers, and advocates is how all communities are run. Digital platforms must embrace this approach since they are virtual communities reflective of society. Every platform has extensive engineering expertise that can be used to help prevent problems online when coupled with the right subject matter experts in a given problem area. While many platforms often donate funds to organizations, this limits the true impact that can happen when subject matter experts, advocacy organizations, and platforms work directly with each other to implement solutions to problems online.
    - **Note**: Platforms often take a check the box approach to working with outside groups. Platforms can create internal positions staffed by experts in various areas that impact society overall such as law enforcement, parents, teens, education, child safety, teen issues, and more. Such internal experts can be a solid touch point for external advocates and policy makers to create long term solutions with real impact.

CONCLUSION

As an expert in online safety, security, and privacy for more than 20 years, I have seen the evolution of efforts that online sites have taken to protect their users. One thing that remains consistently clear is that entities that choose to rely on notice and takedown systems are choosing to put their users in harm's way and choosing to allow bad actors to put a foothold into their platforms. There simply is no other way to look at it. It also remains consistently clear that platforms have developed technology-based and human-based solutions that can be proactively applied in numerous areas related to safety, security, and privacy if the willingness to do so existed. The injuries that have been created and the ills that have resulted from lack of proactive conduct can be reduced and sometimes eliminated by just such proactive solutions, many of which have been highlighted throughout this guide.

About the Author

Hemanshu (Hemu) Nigam has been at the forefront of online privacy, security, and safety for the past 20 years as a federal prosecutor against online crimes and a senior executive running online safety, security, and privacy programs inside platform companies. He has built global programs to create safer, more secure, and privacy friendly environments for users online. Hemu's brings a unique perspective having seen the challenges presented from numerous angles – policy, enforcement, product, government, advocacy, and technology. He recognizes that a proactive, lean forward based solution is a critical part of any program designed to keep users online safe and secure, while preventing the mis-use of such platforms.

Hemu's full bio
hnigam@sspblue.com
310.909.6757

////