INDUSTRY BEST PRACTICES REGARDING THE NON-CONSENSUAL DISTRIBUTION OF SEXUALLY INTIMATE IMAGES

While the Internet has enabled countless advances in education, workforce productivity, consumer services, social networking, and community connectedness, like all technologies, it has the potential to be misused in a variety of ways, including elder abuse, security attacks, fraudulent activities, and harassment. The use of websites, applications, and other technologies to distribute and publicize sexually intimate or explicit images of individuals without their consent and often with the intent to do emotional, financial, or personal harm is one such abuse. The use of the Internet for this purpose is abhorrent to the technology industry and has led many industry leaders to ban the practice and create mechanisms to assist victims. This document aims to chronicle these efforts and provide a broad overview of these practices to help all industry participants adopt best practices in this area.

At the outset, it is important to note that in responding to this abhorrent behavior industry leaders have looked to develop an aggressive response that is mindful of the powers and limitations of technology, while demonstrating their lack of tolerance for this behavior and their commitment to the victims of this abuse. The best practices outlined here are not to be treated as industry standards or best practices for legal purposes or otherwise, indeed the diversity of technologies involved demands flexibility. Instead, this document reflects the participants' abhorrence with this abuse of technology and suggestions as to methods for combatting it, recognizing that that there are technological limits to what the most well-meaning, properly motivated companies can do, and that each company will need to implement practices that reflect the powers and limitations of the particular technology.

The following overarching themes have informed all of the best practices cataloged here.

1. **Target the source**: Efforts to prevent and respond to this behavior should focus on the source – the bad actors who publicly share or distribute the images with knowledge that they do not have consent of the individual(s) depicted, as well as companies that are developing websites and other technologies designed specifically to host, promote, or distribute nonconsensual sexually intimate images. These entities should be rightfully targeted by law enforcement officials for engaging in and encouraging illegal behavior.

2. **Context matters**: The sheer volume of activity enabled by the Internet, including the billions of daily posts, tweets, blogs, e-mails, and uploads generally, as well as the specific need to investigate the context that surrounds this content in order to accurately identify it as a malicious posting in violation of either a company's policies or the law, makes it impossible, both practically and legally, to pre-approve or proactively monitor this content. Therefore, to help eradicate this behavior, industry must focus on best practices for removing reported content.

3. **Technology has limits**: There are technological limits to what the most well-meaning, properly motivated companies can do. For example, search engines do not control content; they only link to content, so whatever steps they take will not actually remove content from the Internet. There are similar limits with other technologies and services. Each company will need to implement practices to deal with this behavior that reflect the powers and limitations of the particular technology.

4. **No "one-size-fits-all" approach**: The technology industry is anything but monolithic. Service providers, content suppliers, manufacturers, platform hosts and the multitude of other industry participants all have to address this issue in a format that works for their own models. We offer this catalog of best practices as examples of the initiatives available to companies dependent on their model, not as a universal best practices document that would be appropriate for all.

BEST PRACTICES

COMMON, INDUSTRY-ADOPTED BEST PRACTICES

TERMS AND CONDITIONS

The first step in working to combat the non-consensual distribution of intimate images is to develop a strong, clear, and readily discoverable policy to address the topic. Policies will vary depending on the nature of the product, good or service provided, but would focus on prohibiting the conduct.

For content providers or hosts, sharing platforms, or social media products, the policy would prohibit the public storage or distribution of intimate images intended to be private on the device, platform, application, or website. There are some differences regarding how such conduct is banned, but the most common policies are typically sub-sets of broader prohibitions on nudity, pornography, or harassment. Policies would be easy to find, clear to follow and understand, and include specific instructions for victims. For violations of the policy, the content would be removed and user-level or even device-level bans for actors that violate these terms would be included.

For search engines and content aggregators, policies would, where possible, focus on assisting the victim of the conduct and reducing the harm. These policies may include removing offending URLs from search algorithms and/or banning content providers that feature these images from aggregator sites and engines.

CONSUMER TOOLS

As a compliment to strong, clear terms of service that prohibit such conduct, best practices would include consumer-facing tools that are easy to access and use, with multiple access points and avenues to report harassment or abuse and to request available remedies. These consumer tools could include:

1. A specific web page on the topic, discoverable from search off a main web page or otherwise designed for ease of access.
2. Specific instructions on content removal and advice on how victims can minimize exposure across platforms and sites.
3. Links to helpful resources for victims.

REMOVAL PROCESS

Given the practical and legal challenges identified above, abuse-reporting and response systems must be complaint-driven. The request-for-removal process would be designed for ease of use and quick resolution; keep the complainant informed of progress, and note target timeframes for resolution. Practices vary, but timelines as short as 48 hours have been adopted with efforts to exceed that expectation. While additional communications may be needed or helpful, a sufficient process would include updates to the complainant during any unexpected or necessary delays and would also include a notice of final resolution.

COMMUNITY OUTREACH

Best practices include consumer and policy maker awareness-raising to increase knowledge and educate the public about the issue, challenges, and difficulties, and to encourage appropriate policy responses and coordination with law enforcement officials. Typical activities, such as stakeholder roundtables, awareness-raising and educational campaigns, non-profit outreach and partnerships, and training activities are all considered valuable community-related activities.

OTHER PRACTICES

VERIFICATION PROCESSES

The complaint process will require a level of verification before images are blocked, removed, or identified as violating the terms of use for a particular company. Some companies have agreed to a self-identification and verification system, which is the easiest for a victim to navigate. Other suggestions include tagging a filed police report as sufficient verification.

RESOURCE SUPPORT

Some companies have budgeted resources to assist victims in understanding their rights, minimizing their exposure, and addressing their issues with webmasters and website operators.

ACKNOWLEDGEMENTS

The following companies contributed to the content and review of this guide: Facebook, Google, Microsoft, Pinterest, Twitter, and Yahoo!

A product of the Attorney General's Cyber Exploitation Task Force
http://oag.ca.gov/cyberexploitation/

##