

How to Responsibly Create Technological Interventions to Address the Domestic Sex Trafficking of Minors

The domestic sex trafficking of minors, also known as the commercial sexual exploitation of children (CSEC), is a serious form of violence that can cause significant harm to youth at great societal cost. Many new communication and information technologies – including mobile phones, social network sites, and online advertising services – fundamentally alter different aspects of the commercial sexual exploitation of children.¹ While technologies change the contours of youth's exploitation, they also create new opportunities to intervene.

Recently, many technologists – including academic computer scientists, entrepreneurs, and engineers in governmental and corporate organizations – have been investigating ways to use technology to address domestic sex trafficking and CSEC. As researchers invested in understanding and disrupting CSEC, the level of interest and passion for innovation excites us. We have written this document to help provide basic information for technologists who are imagining ways to help.

Curbing commercial sexual exploitation of children and promoting the rights and safety of children should be a top priority for all members of society. Yet, all too often, myths and public misunderstandings – particularly about technology's role in CSEC – and a lack of empirical data about the scope of the problem drive political and legal agendas, however well intentioned. These same myths and misunderstandings have the potential to inadvertently affect how technologists approach the problem. As researchers, we feel it's important to take an evidence based and data-driven approach toward technological interventions so that they are effective, efficient, and limit the additional harm done to victims. With this goal in mind, we offer a series of key findings that should be a part of any serious discussion about using technology to address CSEC in a networked world. We hope that this information is useful for technologists seeking to build innovative solutions. We would be happy to offer more detailed information and data to any technologist seeking to learn more.

Understanding the Youth Involved

Social media, mobile apps, and other networked technologies present an unprecedented opportunity to reach out to at-risk youth, victims, and survivors. Doing so requires in-depth knowledge and understanding about youths' needs and youth should be at the center of potential design solutions. Moreover, technologists should resist the temptation to stereotype all CSEC events as identical, but instead understand that CSEC is an umbrella term that refers to a broad array of situations.

Youth often do not self-identify themselves as victims. Different interventions are needed when youth do not see themselves as victims, but as individuals making their own decisions and exercising agency amidst constrained life circumstances, or when decision making is impaired due to substance abuse or mental illness. While many of these youth may not be amenable to being "saved" they remain in need of access to services that can assist them. For interventions to help, it is important to work with youth's understanding of their experiences.

“Survival sex” is one aspect of CSEC. While minors engaged in commercial sex and prostitution may be exploited, not all are exploited by pimps. Youth may find themselves in situations where their financial, mental health, and/or survival needs affect their risk of exploitation. They may also be seeking power and validation. Substance abuse and mental health issues are often complicating factors. Listening to how youth describe their experiences and understanding the nuances of CSEC is important for any intervention.

Previous sexual abuse, homelessness, family violence, and foster care may influence youth’s risk of exploitation. Youth who are victimized may come from vulnerable situations where they have learned to distrust adults and authorities. Lack of meaningful access to social services can increase the likelihood that an at-risk young person will experience exploitation.

Parents and family members can be part of the problem. Youth who are at-risk of exploitation or who have been exploited may come from unstable, unprotective, or abusive households as well as from situations where biological or foster parents or family members are their primary exploiters or facilitate their exploitation. Interventions should not automatically assume that parents are positive actors.

Both girls and boys can be victims. More attention is given to girls, yet boys and transgender youth are also victims of CSEC. Furthermore, lesbian, gay, bisexual, transgender, and queer (LGBTQ) youth, in particular, may be especially vulnerable. Innovators should be cognizant of the diversity of potential youth at-risk, utilize language and intervention models that are inclusive to different gender identities and sexual orientations, and develop solutions that aren’t just targeted at one population.

Many or most youth are in or nearby their home communities. The term trafficked may create the misleading impression that most of these youth have been moved around against their will - or across state or national boundaries - but this is often not the case.

Technology Assisted Law Enforcement

Computational analysis and search capabilities may offer powerful tools to assist law enforcement in locating at-risk youth and the individuals who exploit them. In designing such technological solutions, the following issues should be taken into account:

Law enforcement is not always trusted by youth. Many youth may have had significant run-ins with law enforcement who are often the first to respond to a potential CSEC case. While some of these interactions are positive, many youth do not feel as though law enforcement is on their side or can be trusted. Some work with, or are manipulated by, those who exploit them to avoid law enforcement. In order for technologies enabling law enforcement to reach at-risk youth to be meaningfully effective, agencies need to rebuild trust with those they’re seeking to help.

Arresting victims undermines efforts to combat CSEC. The difficult and challenging circumstances that many exploited youth experience might lead first responders to believe that an arrest – or a night in jail – is a better outcome for them than spending a night on the street. However, arresting youth undermines their trust in law enforcement and can result in criminal records for victims that limit future opportunities for recovery. Rather than helping them, arresting youth can in fact heighten their

vulnerability and risk of violence upon release from detention facilities. Safe harbor laws signal an important step in the right direction. Yet, even in states where these laws exist, youth may be arrested or placed in detention before they are offered social services. Those intervening should be mindful that arrest and criminalization undermine youth's safety.

Technologies should help disrupt criminal networks. It is easier to design technologies that identify unsophisticated offenders who make their acts widely visible or to build tools that surveil and help criminalize existing vulnerable populations. It is harder - but more effective - to target and identify criminal networks and sophisticated criminals. This is especially important since surveillance tactics tend to disproportionately target marginalized populations, including LGBTQ youth and people of color.

Organizational decisions matter. Some police departments and law enforcement agencies have moved away from arresting victims, moving cases to special victims units who are specifically trained on CSEC; unfortunately, many have not. When law enforcement is encouraged to focus on arrests and prosecutions, there is more incentive to go after more visible cases and cases that are easier to prosecute or to use punitive tactics that could be more harmful than helpful. In some jurisdictions, officers may arrest victims or low-level criminals rather than pursuing those actors who are engaged in organized crime or offenders who have high social status. To effectively disrupt CSEC, technologies should help law enforcement with lead generation that helps them prioritize targeting violent offenders.

Broader Provisions

Technologies can also be developed for direct service providers, non-profits, and educators, as well as technology firms whose networks may be used to exploit youth. Yet, the introduction of any technology can also change the ecosystem in ways that complicate successful interventions. In order for technologies to be effective, it's important to make certain that broader provisions are in place.

Post-identification support should be in place before identification interventions are implemented.

In many communities, there are not enough beds or social services to assist youth who have been identified as at risk for CSEC/DMST. In any setting where technology is implemented, there should be a well-understood and coordinated intervention plan that can help victims once they have been identified. This includes medical, mental, and social services as well as a long-term protocol to assist youth. Without such infrastructure, heightened identification as facilitated by technology will offer youth inadequate support and add to the problem.

Collaboration is key. Many of the youth identified through trafficking programs as children at risk of exploitation are the same youth who have been identified by child welfare, drug abuse, school failure, and foster care improvement programs. It is very important that new initiatives incorporate and improve rather than displace or compete with preexisting efforts that have proven effective in serving this population. Those designing technology should partner with these organizations to help design and implement interventions.

Leverage how technology makes CSEC visible to get at the underlying problem. Technologies connect people. This facilitates interactions between at risk youth and individuals who may exploit them,

but it also makes CSEC more visible to broader audiences. While visibility creates new vectors for exploitation, it also creates new opportunities for intervention. Eradicating technologies that make CSEC visible will not solve the underlying issues. Energy should focus on using what's visible to identify criminal activity and help vulnerable youth.

Evaluation, assessment, and accountability are critical for any intervention. The innovation process often thrives on experimentation; technologies are built and tested to see what might work. While this process can be quite beneficial, it is important to always remember that these interventions are affecting people's lives in significant ways. All interventions should be measured as to their efficacy as well as their unintended and/or harmful outcomes; protocols should be put into place to rapidly respond to any potential repercussion.

Efforts need to be evidence-based. A problem such as CSEC is easy to stereotype for publicity purposes, but the actual research on its scope, variety, and dynamics is quite limited. Miscalculated and misrepresented data and statistics will not help the ultimate goal of addressing exploitation. Care needs to be taken to develop collaborative, quantitative, qualitative, and rigorous research as the basis for effective prevention and intervention. Designers of systems should beware of assumptions and focus on formulating testable hypotheses.

The cleanliness of data matters. Technologists are increasingly interested in harnessing "big data" to address CSEC, yet much of the data that they will encounter is quite "dirty." Technology experts should work with domain experts to interpret the data in order to recognize which traces are likely to reflect a CSEC case and which traces may be an indicator of other practices. Some data can be misleading and, without domain knowledge, technologists can easily misinterpret what they see. Technologists need to understand that many insidious traces are encoded and hard to identify.

Cross-sector and cross-expertise collaboration is key. Technology experts should work with researchers, law enforcement agencies, non-governmental organizations, and domain experts to develop technologies and protocols that do no additional harm. It is imperative to be more cautious when trying to build systems that are used to intervene in CSEC situations.

Civil liberties are important considerations. As technology experts and technology firms seek to intervene in CSEC, policies on privacy and data security should be developed with input from experts across sectors.

Technology cannot produce a silver-bullet solution. Technologies create profound opportunities for connecting people and promoting new ways to assist youth. Yet technology alone cannot solve underlying structural forces that render youth vulnerable to exploitation, including poverty, unstable housing, lack of social services, and cracks in the various systems intended to protect them. Technology should be seen as a valuable tool in combating exploitation, but should not be viewed as a complete solution.

We are grateful that technologists are committed to combating CSEC and disrupting the domestic sex trafficking of minors. We hope that this document offers technologists some basic information about how to ethically and thoughtfully proceed with innovative efforts. We would be happy to provide additional information or data should any technologist be interested. All we ask is that those working in this space think carefully about the potential consequences of the tools they build. As researchers and scholars passionate about the people affected in this space, we are all committed to making sure that interventions do no additional harm.

Sincerely,

Christina Bain, Babson Social Innovation Lab
David Blair, Georgetown University
danah boyd, Microsoft Research and New York University
Nicole Bryan, Montclair State University
Dawne Clark, Mont Royal University
David Finkelhor, University of New Hampshire
Kirsten Foot, University of Washington
Stepanka Korytova, Indiana University-Bloomington
Mark Latonero, University of Southern California
Mary Leary, Catholic University of America
Phil Malone, Harvard Law School
Kimberly Mitchell, University of New Hampshire
Jennifer Musto, Rice University/Wellesley College
Susan McIntyre, The Hindsight Group
Sasha Poucki, Montclair State University
Anna Shavers, University of Nebraska
Mitali Thakor, Massachusetts Institute of Technology
Sriyani Tidball, University of Nebraska
Janis Wolak, University of New Hampshire

April 8, 2013

To follow-up, feel free to contact: danah boyd <dmb@microsoft.com>, Mark Latonero <latonero@usc.edu>, or Jennifer Musto <jmusto@wellesley.edu>

¹ To learn more about how technology changes domestic child sex trafficking, see reports produced by the *University of Southern California's Annenberg School* at: <http://technologyandtrafficking.usc.edu/>