Understanding the role of technology in the commercial sexual exploitation of children: the perspective of law enforcement

Kimberly J. Mitchell, Ph.D.
danah boyd, Ph.D.

November 2014

Highlights

This exploratory study was conducted to better assess how technology can be used in criminal investigations; it is important to get a better understanding of how technology is currently employed in child sex trafficking as well as the approaches and needs of law enforcement. 144 investigators from Internet Crimes Against Children (ICAC) Task Forces and affiliate agencies responded to an online semi-structured survey, including 45 investigators with experience conducting investigations of the commercial sexual exploitation of children (CSEC) that involved technology. Participants included investigators working in local, county, and state law enforcement agencies in the United States.

The discussion suggested a great deal of variation in perspectives and experiences surrounding the problem of CSEC and technology. Investigators were able to highlight both benefits and obstacles. Benefits included the availability of digital evidence instead of relying on personal accounts, the monitoring capabilities of police, and the ability to conduct extensive undercover operations. Obstacles tended to focus on financial concerns, the continual need for training and technical assistance, and the rapidly changing technological environment.

Findings highlight the vast complexity and variability in these crimes. There is still quite a bit of the unknown when it comes to investigating CSEC – technology changes rapidly and avenues for marketing and communicating are vast. Continual education, training and technical assistance are central to investigators’ needs in this area.
About The Authors

**Kimberly Mitchell, PhD** received her Ph.D. in Experimental Psychology, with a concentration in Quantitative Methods, from the University of Rhode Island. For over 15 years she has conducted research about youth Internet victimization, youth exposure to violence, and sexual exploitation of minors. Dr. Mitchell has considerable experience with law enforcement surveys and studies of CSEC. She was co-Principal Investigator on the 1st and 2nd National Juvenile Online Victimization Studies and the 1st National Juvenile Experience with Prostitution Study. She also received a grant from the Department of Justice to investigate how technology is involved in CSEC and a gift from Microsoft to explore the role of technology in human trafficking. She was directly involved with the 1st and 2nd Youth Internet Safety Surveys; and was Principal Investigator on the Survey of Internet Mental Health Issues, a survey of mental health practitioners, and the 3rd Youth Internet Safety Survey, funded by OJJDP. She is currently Principal Investigator of a NIJ grant aimed at improving current policy and practice on technology-based harassment victimization by examining it within the context of other types of youth victimization, risk, and protective factors. Findings from Dr. Mitchell’s research have been used to help build a knowledge base around the epidemiology and risk factors for critical adolescent health concerns, including CSEC and other forms of sexual exploitation. Dr. Mitchell is the author of over 70 peer-reviewed papers, including publications in the *Journal of the American Medical Association, American Psychologist, Pediatrics, Journal of Adolescent Health*, and *Professional Psychology: Research and Practice*.

**danah boyd, PhD** is a Principal Researcher at Microsoft Research, a Research Assistant Professor in Media, Culture, and Communication at New York University, and a Fellow at Harvard’s Berkman Center for Internet and Society. She is also the founder and president of a think/do tank called the Data & Society Research Institute. Her research examines the intersection of technology and society with an emphasis on “big data,” privacy and publicity, and youth culture. Her 2014 book - "It’s Complicated: The Social Lives of Networked Teens" - has received widespread praise from scholars, parents, and journalists.
# Table of Contents

Introduction .......................................................................................................................................................... 4

Definition .......................................................................................................................................................... 5

Current study .................................................................................................................................................. 6

How this study was conducted .................................................................................................................. 6

Main Study Findings ..................................................................................................................................... 8

  Has Technology Changed the Dynamics of Sex Trafficking Cases? ...................................................... 8

  What is Unique about Child Sex Trafficking Cases involving Technology? ...................................... 10

Types and Ways Technology is Being Used by Traffickers .................................................................... 12

Special Issues – Niche Sites and Encoded Language .............................................................................. 14

Using Technology to Help Victims ........................................................................................................ 14

Opportunities and Obstacles Afforded by Technology .......................................................................... 15

Biggest Concerns about the Use of Technology by Child Sex Trafficking Criminals .......................... 16

Needed Resources ....................................................................................................................................... 17

Conclusions .................................................................................................................................................. 20

Recommendations ..................................................................................................................................... 20

About the Crimes against Children Research Center ............................................................................. 21

Acknowledgements .................................................................................................................................... 23

References .................................................................................................................................................... 22
Introduction

Many children and adolescents are sexually victimized in violation of criminal statutes and societal values. A national study of youth (ages 2 to 17) revealed 2% had experienced sexual victimization in the past year and 5% in their lifetime.\(^1\) Additionally, the National Crime Victimization Survey showed that, in 2009, the overall violent crime victimization rate for teenagers (ages 12-15) was more than twice the average national rate.\(^2\) Child sex trafficking, also known as the commercial sexual exploitation of children (CSEC), is a particularly egregious subgroup of sexual victimizations because, in addition to being sexually abused and assaulted, victims are treated as commodities and abused for financial and economic gain. Although the dominant narrative of child sex trafficking involves criminal networks profiting from trafficking underage victims over long distances for sex or for the production of child pornography, the dynamics of this crime can often be far more complex. For example, often correlated with histories of abuse, poverty, and/or mental health struggles, some minors knowingly engage in sex work to escape or survive. These vulnerable youth are still criminally exploited, but the dynamics of the crime and interventions needed are quite different from those who are abducted or exploited by mediators seeking to profit off of them.

Technology and child sex trafficking

Many types of social activity now involve technology, so it should not be surprising that this is true for crime in general and commercial sexual exploitation and trafficking in particular. This means, of course, that efforts to prevent and prosecute exploitation-related crimes require a sophisticated understanding of the Internet and other technologies as well. Child protection and criminal investigators, however, do not always know how to effectively leverage technology. More research and practice is warranted to develop better methods to identify, investigate, prevent, and intervene in child sex trafficking in all its forms.

Empirical research on child sex trafficking is almost non-existent, and summaries of case characteristics and ways that technology is involved in such cases must rely on legal reports and media stories\(^3,4\). These stories suggest that criminals involved in trafficking and those facilitating juvenile prostitution are making use of online resources. The Internet provides a way to advertise anything to wide audiences, including escort services and massage parlors. Adolescents may be marketed or market themselves in such places alongside adults. Online dating sites, intended to enable mediated introductions between consenting adults, can be repurposed to power commercial sex, including the exploitation of minors. Even the most popular social media, designed to enable friends to connect and share, can be used for illicit purposes. Technology may also provide an efficient means of reaching obscure target audiences - including immigrant groups that may be the focus of international traffickers, pedophiles looking for access to very young children, people with abuse-oriented sexual tastes, and those interested in child pornography.

How those engaged in the commercial sexual exploitation of children use technology in their trade may vary. Those engaged in illicit activities may believe that technology offers ways to hide criminal
activities. Some assume anonymity or do not understand the traces that they leave behind. Others take measures to obfuscate their online activities, for example by encrypting communications and picture files and using wireless technologies that may be difficult to trace to specific locations. In addition to advertising trafficked victims, exploiters may use communication platforms to make connections with other offenders, for example networking among pimps or with child pornography rings. They may also use basic commercial tools to address the business side of trafficking, turning to online banking for money management or ordering clothes and other goods for victims. Finally, technology may also be used by youth who are engaged in sex work on their own in order to advertise their services and find clients.  

*Technology, trafficking, and law enforcement*

At local, county, state, and federal levels, law enforcement officers investigate and prevent commercial sexual exploitation. Although the relationship between law enforcement and those who are sexually exploited can often be fraught, many law enforcement officers are conscientiously seeking to minimize exploitation. Some focus specifically on child abuse; others are focused on trafficking writ large; still others encounter commercial sexual exploitation as part of other investigations that they conduct. The use of technology in child sex trafficking cases can pose both benefits and challenges to how law enforcement investigates these types of cases. In some senses, the practices surrounding trafficking are more visible because of the traces left behind by criminal activity. At the same time, these traces are not always easily identifiable or interpretable, rendering them less visible than they would be in more traditional settings.

*Definition*

The term “child trafficking” is ambiguous and often inconsistently defined. Under the Trafficking Victims Protection Act of 2000, human trafficking has occurred if a person was induced to perform labor or a commercial sex act through force, fraud, or coercion. Any person younger than 18 who performs a commercial sex act is considered a victim of human trafficking, regardless of whether force, fraud, or coercion is present. The language defining sex trafficking appears to refer specifically to crimes that a third-party exploiter (e.g., a pimp) who profits from the involvement of the youth in prostitution commits. However, the distinction between prostitution and trafficking has been debated. Furthermore, the term “trafficking” often implies that someone moves youth involved in prostitution. Not only are many youth on their own, but even those with third-party exploiters often remain in their community of residence and are not taken across state or international borders. In the United States, the organized movement of youth from community to community for sexual purposes appears to apply only to a small segment of the youth identified as involved in prostitution, according to criminal justice data.

For the purpose of this study we consider CSEC to be cases involving sexual offenses against children or youth in which there was an exchange or an effort to exchange money, and the exchange clearly occurred so that at least one party would profit financially. This definition excludes child pornography trading, sexual exchanges for nonmonetary gains, and money offered to victims as a bribe or incentive in an otherwise noncommercial sexual assault. This narrower definition focuses public and professional attention on the relatively small but high-risk category of child sexual
victimization cases where financial profit is involved. A broader definition may aid those seeking to draw attention to the scope of the problem, but it may have the unfortunate consequence of distracting and confusing law enforcement efforts: the large number of child sexual victimization and child pornography cases with no clear financial or profit-making element would overwhelm the smaller numbers of more serious CSEC cases. A too-broad definition could also increase the risk that sexual assault victims are given potentially harmful labels such as “prostitute.” Likewise, all-encompassing definitions complicate professionals’ and researchers’ efforts to understand the unique characteristics and consequences of CSEC crimes to better target intervention and prevention activities.

We used the term “child sex trafficking” in the survey to respondents due to its widespread use among professionals and to help facilitate discussion on this topic. Child sex trafficking was defined as sex trafficking involving minors under the age of 18 by being sold or bought for sex, including victims exploited by pimps and minors acting on their own, both boys and girls.

Current study
To better assess how technology can be used in criminal investigations, it is important to get a better understanding of how technology is currently employed in child sex trafficking as well as the approaches and needs of law enforcement. As such, Microsoft funded the Crimes against Children Research Center (CCRC) at the University of New Hampshire (UNH) to conduct an online survey of ICAC Task Forces and their affiliate agencies. This white paper describes the experiences and opinions of 144 investigators who responded to the survey.

The goals of the survey were to explore:

- Law enforcement’s understanding of how technology is being used in child sex trafficking by exploiters to advertise and sell victims
- How underage victims market themselves in sex trafficking cases seen by investigators
- How those seeking to pay to sexually exploit minors may use technology to locate and purchase victims based on existing cases
- How law enforcement investigates technology-involved sex trafficking cases
- The opportunities and obstacles presented by technology in performing law enforcement work
- Investigators’ needs as they seek to successfully investigate child sex trafficking cases with a technological component

How this study was conducted
Data was gathered from law enforcement investigators working with the ICAC Task Forces. A link to an online survey was distributed by email in November-December of 2012 to all commanders of the ICAC Task Forces (n=61) and contacts for ICAC affiliate agencies (n=3,739), a total of 3,800 law enforcement agencies. Acknowledging the work load and time considerations of law enforcement we aimed to reach a total of 150 investigators about their experiences in this area. We received responses from representatives from 38 ICAC Task Forces and 106 affiliate agencies (n=144) by the close of the survey.
The ICAC Task Force program was created to help state and local law enforcement agencies enhance investigative responses to offenders who use the Internet and related technologies to sexually exploit children. The program includes regional ICAC Task Forces in every state and affiliates, which are partner agencies that have agreed in writing to adhere to ICAC Operational and Investigative Standards.

Names and email addresses for each of the ICAC Task Force directors and their affiliates were provided by the ICAC Training & Technical Assistance Program staff. This information was uploaded into a web-based data collection program called Vovici. This program is a multi-functioning survey tool that allows the user to create a data collection instrument and organize a participant list, and also hosts the data in a secured environment. Participants received one email reminder if they did not complete the survey within 2 weeks of invitation and a second email reminder 2 weeks after the first.

The online survey asked whether the respondent had investigated a child trafficking crime. If yes, they were directed to a series of questions which asked for general details about how technology was used in the respondent’s investigations of child trafficking cases. Additionally, in order to assess law enforcement needs in this area, all participants, regardless of whether or not they had investigated such a case, were asked a series of questions about law enforcement needs for investigating and combating child sex trafficking. For example, we asked all participants 1) their biggest concerns about the use of technology by child trafficking criminals, and 2) the resources, training, and technical assistance that they believe will be necessary over the next decade for investigating technology-involved trafficking cases. All procedures were approved by the University of New Hampshire Institutional Review Board.

Responding agencies included local, county, and state law enforcement agencies.

- 27% served small jurisdictions (populations of 25,000 or less)
- 32% served medium-sized jurisdictions (populations between 25,001 and 100,000)
- The rest, 42%, served jurisdictions of over 100,000

The individuals who responded to the survey were commanders or investigators from ICAC Task Forces and affiliate agencies; 76% were men. 81% worked for a particular unit in their agency: 49% worked for a crimes against children unit, 33% for a sex crimes unit, 40% for a computer crimes unit, and 34% for some other unit (multiple responses were possible).

Participants had a wide range of experience with investigating crimes against children. Among all responding investigators:

- Almost all investigators (92%, n=133) had investigated crimes against children. Of these, 45% investigated crimes against children “all of the time,” an additional 41% did so “sometimes,” and 14% did so “rarely”
12% of investigators who had ever investigated crimes against children had been doing so for more than 20 years, 29% for 11-20 years, 32% for 6-10 years, and 26% for 5 years or less.

31% (n=45) of all respondents had investigated at least 1 child sex trafficking case during their career. Of these, 18% had been conducting such investigations for more than 10 years, 31% for 3-5 years, 49% for 1-5 years, and 20% for less than 1 year.

This white paper contains information about the investigation of child sex trafficking crimes from these 45 investigators, as well as information about the obstacles, needs and concerns about the role of technology in child sex trafficking investigations from all 144 respondents. In addition to demographic data about themselves, respondents were asked a series of open-ended questions about their experiences. In reporting on the qualitative data, we use exact quotes provided by law enforcement officers. We analyzed the qualitative data to identify both trends and diverse perspectives; the quotes provided are intended to reveal the range of viewpoints that we heard, while we highlight repetition of perspective through our descriptive discussion.

Main Study Findings

Has Technology Changed the Dynamics of Sex Trafficking Cases?

In the experiences of law enforcement investigators, technology is commonly a component in sex trafficking in some capacity. Among investigators who have investigated a child sex trafficking case, over half of investigators (69%) said that most of their sex trafficking cases (76 – 100%) involved technology in some way; a total of 80% said over half of their sex trafficking cases involved technology. When technology is involved, it plays a very (33%) or extremely (60%) important role in the case.

This is perhaps not surprising given the ubiquitous nature of technology in today's society. The Internet has changed the way societies function; and at the same time, it is an emerging environment that lacks traditional boundaries. Indeed, new technology has transformed how youth communicate with each other and relate to the world. Technology is ubiquitous: 95% of youth use the Internet,11 73% use social media sites,12 77% own a cell phone,13 and 72% of teens frequently text their friends.13

In light of the broader societal shifts, investigators described ways they feel technology has changed the dynamics of child sex trafficking cases. Two common themes that emerged in their responses were that technology provided access to a larger pool of clients and that it made marketing easier.

Larger pool of clients

"Allows for greater access to more potential predators and assists in documenting the contact."

UNIVERSITY of NEW HAMPSHIRE
“It increases access to a vast pool of clients and yes it does speed up negotiation.”

“More people using the internet, more social networking cites (sic). The offenders always seem to know the sites before the Police do.”

“Probably increased the pool of clients as well as the ability to communicate with a multitude of people very quickly either by cell phone, text messaging and e-mails. This includes the ability to share photos which can be a big component to these cases.”

**Made marketing easier**

“It has created a "one-stop-shopping" opportunity for the offenders. They can find locations and pimps, make arrangements and "preview" the desired victim all from the comfort of their own home.”

“Technology has made marketing easier and lowered the barrier to entering the business, especially for pimping and pandering. Camera phones and file sharing websites also facilitate criminal activity.”

“Ease of access through the web. Clients have access to pictures and telephones numbers of girls and the negotiation is very fast.”

“Large market place, the ability for clients to be more discrete, and most difficult in tracking and monitoring online posts due to the amount of posts and ability to delete posts rapidly.”

For many law enforcement respondents, technology unquestionably makes exploitation easier by enabling efficient forms of communication, increasing the scale at which abusers can operate, and making access available to a larger pool of potential victims. What respondents struggle with is how it helps or hinders their efforts to combat child sex trafficking and the relationship between this crime and other crimes. For example, one respondent noted that not only did the Internet increase anonymity, “It also spreads the child pornography images/videos faster and worldwide.”

Law enforcement officers see technology as pervasive and central to commercial sexual exploitation. As one respondent explained, “Almost everyone being prostituted is advertised on some type of advertising or social media site.” This same officer continued on to highlight that this can be beneficial in the pursuit of criminal activity, noting, “It does make it easy for us to find targets or put up our own undercover ads to look for offenders.”

Even as respondents raised concerns about the ease with which traffickers could use technology and difficulties officers faced in being proactive in this new medium, many, like the aforementioned respondent, simultaneously highlighted the potential for leveraging the data traces left behind by traffickers. Some investigators lamented the limitations of policing or questioned whether or not law enforcement could keep up with exploiters’ ability to utilize new modes of communication and exploitation, but others saw new opportunities for engaging in policing work. This tension is at the core of the conversation happening around technology’s disruptive dynamics.

These dynamics are not unique to Internet-based technologies. Guns, automobiles, and telephony also simultaneously aided and hindered law enforcement officers' efforts to combat criminal
activity. And new technologies are used in most types of crimes, not just commercial sexual exploitation. One respondent explicitly stated, “Over the past couple of years cell phones have become involved in every crime. Sex trafficking is no different.” What’s notable about the Internet as it relates to commercial sexual exploitation stems from the ways in which it uniquely alters the practices of observation, data collection, and sting operations.

What is Unique about Child Sex Trafficking Cases involving Technology?
We asked investigators who had worked on technology-involved child sex trafficking cases what they felt was unique about these types of cases. Most responses focused on benefits to offenders, including increased safety (less risk of detection) for the offenders involved, ease of negotiations and money exchanges, and easier advertisements of victims.

“It creates a safer place for sex offenders to make contact with children of all ages.”

“The up-front risk of detection of the offender is no longer a deterrent and the communication is all real time”

“lower risk to the pimp; makes him/her harder to identify.”

“Transfer of funds, agreement on transaction locations and costs are all easier. Probably the same for stolen property, narcotics and terrorism.”

“The victims are moved from place to place and the ads on webpages make it easy for them get clients.”

“greater distances can e covered to find potential suitors”

One investigator highlighted that what has changed stems from the communication methods:

“The crime is the same, the way they communicate to commit the crime has changed”

A different investigator noted the benefit to investigators from an evidence gathering perspective:

“It leaves a digital footprint of evidence that can be followed. While technology has increased the opportunities for these victims to be offended against, it has also opened up opportunities for these victims to be identified and contacted more quickly.”

While another mentioned the benefits for undercover operations:

“Developing some depth to the undercover profile that is believable. (facebook, myspace, etc)”

What is notable about these responses is that they all focus on qualitative or quantitative shifts in existing practices of exploitation and investigation. In other words, it is not so much that technology introduces unique dynamics as much as it alters the underlying equation of how law enforcement operates.
We first asked investigators at what point they knew when an online advertisement was a sex trafficking case. More specifically, we were interested in understanding what they look for. Through this, we learned that a combination of domain expertise and assumptions about what characteristics to look for were central to those who believed they had the knowledge to proactively investigate. Meanwhile, others highlighted that they only investigated cases reactively, suggesting that it was difficult if not impossible to tell ahead of time.

**Tracking known websites**

“Certain sites are exclusive to that trade.”

“When it’s on a web site or text site commonly known for trafficking kids.”

**Monitoring specific characteristics of websites or advertisements**

“There are some common characteristics in the “ad” photos that will help to indicate what is going on as well as “buzz” terms.”

“Monitoring the webpages and similarities in page layout. Many have the same text, phone numbers, and subpoena records show similarities to email addresses and names.”

“When the ad is cryptic and generally charge more for the encounter. When they don’t specify who the worker is.”

“Whenver it involves sex, dates, or companionship in exchange for monetary compensation or something similar”

**No way of knowing – work reactively**

“You really don’t know until you investigate.”

“Mostly answer complaints.”

“This is the hardest part of the job. When looking at the ad’s posted, the pictures usually are not that of the actually person who shows up. So it’s a case by case event whether or not a child or an adult will be showing up.”

“You can’t, that is the problem, law enforcement is reactive. Usually the pimp will use a different picture in the advertisement than the actual victim.”

Although a few responses highlighted more sophisticated technologies like face recognition, it is notable that most responses provided by law enforcement officers revealed the manual and human-centric nature of using technological tools. Rather than designing and implementing algorithms to automatically monitor sites or advertisements, these officers approached technology as akin to physical sites that they would monitor. In other words, these respondents did not seek out ways of using technology to increase the scale of their own operations even as exploiters did.
We also wanted to know what investigators did once they identified an online ad for sex with a minor. We asked respondents how they went about investigating what they found. Some focused on the organizational and interpersonal processes involved, emphasizing relationships with partner agencies or seeking to make contact with the offender as part of an undercover investigation. Others emphasized technical approaches focused on using the tools to obtain more information.

**Organizational and Interpersonal Processes**

“Start with checking Federal, State, and local partners. Begin undercover contact.”

“Pose as a customer, arrange for an appointment, utilize a neutral meeting area (hotel room, etc), have video surveillance, conduct operation and ultimately arrest involved. Report to human trafficking Fed units if multijurisdictional.”

“Line up a date and try to get them to respond. Usually some communication online and then setting an appointment to meet.”

**Technical processes**

“Identify the originating IP address”

“I monitor that ad and try to identify the locations, phone numbers and need to work quickly before they move to another city. Subpoea (sic) the webpage to get as many identifiers as possible as quickly as possible.”

“Start working backwards as to who posted the ad where and when.”

Although it is likely that all law enforcement officers use a mix of organizational, interpersonal, and technical data collecting approaches in their investigations, the varying emphasis is important to consider. More work is needed to better understand exactly what steps investigators take, what tools they employ in each step, and what forms of collaboration are most effective. The organizational and interpersonal facets, as well as the conceptual maps that law enforcement officers maintain, cannot be easily automated.

**Types and Ways Technology is Being Used by Traffickers**

Although our focus was on understanding law enforcement practices, we wanted to better understand what law enforcement officers knew about the practices of exploiters. In particular, we wanted to better understand the technical practices of those that they identified as pimps. They highlighted three main technologically mediated practices: a) advertising victims, b) interacting with johns, and c) interacting with victims.

Advertising sexual services

Law enforcement surveyed believe there to be a variety of types of technology used by trafficking criminals to advertise children for sex. Law enforcement officers reported investigating cases involving a wide variety of everyday communication platforms: 27% had investigated cases
involving social network sites, 14% had at least one case involving instant messaging, 13% involving email, and 13% involving SMS or text messaging; 17% had investigated a case that involved underground communication channels. One in four (24%) investigators noted cases involving cell phones more generally while 10% specifically noted smart phone apps. Investigators also noted involvement of technology such as information sharing services like online classifieds (24%), niche websites (16%), and search engines (8%) as playing a role in a sex trafficking case they had investigated. Traffickers did not limit themselves to one type of technology and neither could investigators.

An indication of technology affording offenders a “safer” environment to traffic minors could be reflected in how children are advertised for sexual activities. We asked police if the ads they have seen during their investigations of sex trafficking a) overtly portrayed minors for sex, and b) whether minors tended to be advertised as adults or minors. Police told us that the advertisements for minors they have seen are typically hidden in some fashion: only 7% of investigators said most of the ads they have seen overtly portray the fact that minors are for sale. Investigators more commonly found sex trafficking ads where minors were portrayed as adults and thus covert in their intent to sell minors for sex. Clearly offenders are still taking steps to hide the fact that they are engaging in criminal activity, not unlike the use of false identification and attempts to make teens look like young adults when on the street. Technology does not appear to afford criminals complete anonymity or even necessarily a “safer” environment from which to work as we might assume.

Research has also noted the existence of minors who work alone, offering themselves for sexual services, typically to people they do not know, in exchange for money. Here the initiative comes more from the youth, but a youth who may be under varying degrees of desperation because of personal circumstances. We wanted to see if investigators noted any differences in their investigations where minors were apparently working on their own versus under the control of a pimp or other exploiter in terms of the types of technology used and how overt they were about their age in advertisements. In both regards we found the same pattern as when adults were controlling the minor: multiple types of technology being used and minors typically advertising themselves as adults. Even here we see the awareness of CSEC as a crime, even from vulnerable youth themselves.

**Interacting with victims**

Over 3/4 (77%) of investigators said the victims in the technology-involved CSEC cases they have seen were mostly girls; only 2% said mostly boys and 11% said the victims were equally boys and girls (9% not sure). 93% of investigators said the victims in the cases they had seen were mostly teenagers, but police had seen younger children during their investigations as well (7% had seen technology-involved CSEC children under 3 years old, 9% 3-5 years old, 20% 6-12 years old).

Although the current study found more girls in police reports of technology-involved CSEC, research has certainly documented commercial sexual exploitation of boys as well as girls, the majority of which involves adult male exploiters. The predominance of girls noted in this study may simply reflect a law enforcement focus. The age ranges likely reflect the diversity in types of CSEC crimes coming to police attention and not necessarily any indication of the role of technology.
per se. CSEC cases can be classified into at least three categories, each bringing some unique dynamics to the crime: a) cases involving third-party exploiters, such as pimps; b) cases involving minors acting on their own; and c) conventional child sexual abuse cases that involve payment. More male juveniles tend to be involved in the solo and child sexual abuse cases. Child sexual abuse cases also more commonly involved younger, White youth who lived in non-urban areas. Given disconnects between reports focused on identifying victimized youth and those focused on analyzing legal cases, there may be a bias in which cases get reported, investigated, and prosecuted.

Pimps involved in trafficking can use technology to communicate arrangements to victims. The most common avenue seen by police is through cell phones and text messaging. Pimps can also use technology to monitor encounters (51% of police noted this) and control victims (noted by 50% of police).

**Special Issues – Niche Sites and Encoded Language**

Investigators said the victims they have seen exploited via niche sites were sometimes different from those advertised in "adult services" online classified sites (10% of investigators, 68% not sure). One in three investigators (30%) said they had seen cases involving pimps who use encoded language to designate minors (23% not sure). In these crimes, the use of encoded language is at least somewhat common (72% of police).

It is important to remember that most pimps and other exploiters are not sophisticated in how they use technology. For example, people talk about “tech savvy” criminals, but using Facebook or online advertising services is not advanced technological behavior. There is increasing use of technology in every segment of society and for just about every purpose. Millions of people use technology to advertise, post photographs, conduct financial transactions, form interest groups and recruit members, and create and use “members only” sites. Backpage.com is a good example. It is not that innovative. It is called “backpage” because it mimics the advertising that used to be found in the back pages of tabloids sold in cities all across the country.

**Using Technology to Help Victims**

Too often, professionals focus exclusively on identification of dangers associated with technology. While this is critical in raising our awareness to issues relevant to today's youth, it is also vital to focus on how technology can be utilized as a tool for reaching and helping hard-to-reach populations, including youth who are at-risk for or are involved in commercial sexual exploitation. Much has been learned in the past several years about how to help children avoid risky or unhealthy behaviors through the development of innovative technology-based prevention and intervention. Technology-based prevention in the area of HIV risk has been at the forefront of such research with efforts also identified in the fields of drug use and homelessness, all areas of relevance to youth victims of commercial sexual exploitation. We need to work with at-risk youth to create technologies that enhance safety and health and put them in the hands of victims.

Advocates providing services to very high-risk youth struggle with similar obstacles: trying to help youth who are mobile; who have multiple health, mental health and safety concerns; and who come into contact with the system in hard-to-predict patterns. New technology is being used to enhance contact with these high-risk populations in potentially unique and innovative ways. For example,
National Safe Place program, an outreach and prevention program for runaway and homeless youth, launched a text messaging campaign to connect youth with a safe and trained adult in their community at any time and in multiple locations. Agencies working with teen sexual assault and dating violence victims have begun experimenting with web-based, anonymous online chat and text messaging services to provide assistance to victims. Interventions such as these hold promise for increasing assistance to child trafficking victims.

In the current study, 14% of police had seen cases where victims of child sex trafficking were able to use technology to their benefit to: contact help (13%), find services (11%), escape (8%), find shelter (6%), and keep safe (2%). These are examples of what police have seen, that given how important technology is in the lives of youth, the expanding utilities of mobile technologies may be particularly useful for children who lack a solid home environment.

Opportunities and Obstacles Afforded by Technology

When addressing technology's role in child sex trafficking crimes, investigators were able to highlight both benefits and obstacles. Benefits included the availability of digital evidence instead of relying on personal accounts, monitoring capabilities of police, and the ability to conduct extensive undercover operations. Obstacles tended to focus on financial concerns, the continual need for training and technical assistance, and the rapidly changing technological environment.

Most investigators felt that technology has created opportunities for law enforcement in child trafficking investigations that did not previously exist. These include:

- the benefits of digital evidence (85%)
- monitoring capabilities (62%)
- opportunities for undercover work (48%)

Police are using sophisticated technology to respond pro-actively to child sexual exploitation crimes generally and child pornography in particular. Social media and online advertising sites provide evidence and leads. Cell phones, computers, and other electronic can be beneficial for police. They can provide documentation for financial transactions, photographs, communications, physical locations, online histories, searches for information, and more. Prosecutions of technology-facilitated sex crimes against children are quite successful, typically resulting in a guilty plea. More victims are believed; more offenders are convicted.

Obstacles were also noted, however. The key obstacles for the investigation of child sex trafficking when technology is involved include:

- rapidly changing nature of technology (63%)
- lack of available personnel (59%)
- lack of monetary resources (54%)
- lack of age verification of victims (49%)
- lack of training to use technology (44%)
- lack of necessary technological tools (43%)
- difficulty identifying cases as involving sex trafficking (40%)
- lack of victim cooperation (29%)
- inability to prosecute these crimes (15%)

**Biggest Concerns about the Use of Technology by Child Sex Trafficking Criminals**

Investigators of child sex trafficking cases were asked about their biggest concerns about the use of technology by sex trafficking criminals. Most of their responses center on the ways in which technology scales existing dynamics or introduces new dynamics that law enforcement officers do not feel equipped to address.

**Expanded access to victims for offenders**

“Ability by perpetrators to span large distances and involve multiple parties, to the extent that it outstrips the capabilities of many agencies.”

“Ability to locate victims online.”

**Technological advances**

“As things move to the "cloud" more it will be harder to get to the digital evidence we need. Having a hard drive in hand will be a thing of the past.”

“Child sex trafficking criminals can remain anonymous by falsifying or "spoofing" IP addresses or using public WiFi resources to remain anonymous.”

“The use of "throw phones" or drop phone where no identification is required for activation.”

**Lack of investigator time, resources, and training**

“Finding time to monitor social networking activity.”

“Having the time and resources available to properly investigate and to be proactive.”

“Keeping up with the advancement of technology.”

“Lack of personnel and training.”

“Proper documentation and training from experienced instructors who have gone through the process in court and can show proper documentation history for the cases.”

**Working with prosecutors**

“The prosecutors do not understand it and are reluctant to prosecute these cases. In several of these if they could not get a plea they just dropped the case.”

And one investigator explicitly noted the advantage of offenders over investigators when it came to technology by highlighting concerns over "Criminals advancing faster than law enforcement." While new technologies do not inherently need to benefit criminals more than law enforcement, many law
enforcement officers do not feel as though they have the skills, capacity, resources, or laws needed to effectively do their job in this environment.

These concerns about technology need to be understand in the context of research that indicates child sexual abuse is declining; victimization of minors in CSEC is probably also declining. Increasing use of technology by criminals does not mean increased victimization. Every case of child exploitation is a matter of concern, but CCRC research suggests that technology has not increased sex crimes against children. In fact, data from multiple sources indicates that child sexual abuse has declined substantially since the mid-1990’s, and that child well-being has increased 18.

**Needed Resources**

Law enforcement officers reported that they need a variety of resources including, notably: a) financial support and funding, b) training and technical assistance, c) changes in specialization, d) collaboration among agencies and partners, e) help keeping pace with technology, and f) changes to legal mechanisms to investigate and prosecute cases. These are often intertwined since, for example, funding is often identified as critical to gaining access to other types of resources.

**Financial support and funding**

“Financial support for the agencies to fund the proactive investigations. The financial support would be for the investigators pay and for training.”

“Adequate funding, selection of appropriate personnel, focused intensive training and current equipment.”

“Federal funding will be needed to be able to develop training programs. It will also be needed to attend training, to fund investigative activity and to hire personnel.”

Some respondents highlighted that their organizations are actively involved in training. For example, one said, “We have the opportunity to train our own proactive investigators. We allot two (2) to four (4) hours per month for our own little in service. This could cover new programs that pedophiles are using or new websites that we are seeing popping up.” Another signaled that this is built into their organization: “Our office has hosted a statewide law enforcement summit (training for officers) for ten years. Topics have included training on technology crimes and crimes against children.” Still, many more highlighted the need for more training and technical assistance.

**Training and technical assistance**

“Interviewing training and understanding the criminal will always be important. Unencrypting deleted files, especially on iPads and Apple products, will require technical skills. It is very tough to predict the technology needs in two years, ten years is.”

“In-expensive or free training so smaller agencies can get more on board with ICAC crimes.”

**UNIVERSITY of NEW HAMPSHIRE**
“Technical support, training, and cooperation from Internet Service Providers, Cell Phone Services Providers, Social Network Website Administrators, and even computer / cell phone hardware manufacturers will play a key role in helping law enforcement work.”

“Digital forensics along with online support for help in new digital evidence not yet encountered. This includes smartphones, tablets, texting recovery capabilities, industry assistance (ex: instagram, facebook, etc).”

“Continued training for awareness (public and law enforcement), up-to-date training for law enforcement in technology, interviewing, and investigation.”

“More awareness training for basic police recruit training. More integration of uses of technology in investigative training. Creation of support units at the local level, funded by local tax dollars, to assist law enforcement.”

Although most respondents believed that more training was needed, the specifics of what training should look like differ tremendously. Cost is clearly a barrier, particularly for smaller agencies who felt as though they could not afford to develop expertise or train specialists. Some law enforcement officers highlighted that all officers should be better trained in using technology while others focused more on having specialists with specialized technical skills. In general, the tension between general knowledge and specialization shaped a lot of respondents’ understanding of how to best navigate some of these issues.

Changes in specialization

“More forensic examiners.”

“Having a person specifically assigned to investigate these cases. For example, I only occasionally work a computer related case and it is impossible to keep up with the changing technology.”

“de-specialize the training and technical resources, so crimes can be investigated effectively by patrol.”

“Agencies willing to commit personnel for the sole purpose of working these crimes.”

“need an increase in personnel that can recover data from smart cell phones.”

Part of the challenge for law enforcement officers is that they struggle to keep pace with new technologies, be it training, technical assistance, or the need for increased specialization. As one respondent explained, “Keeping pace with the technology would be first. The inadvertent and possibly unintended consequence of advances in privacy software will make it difficult to detect evidence necessary for a conviction.” Yet, it is not just the technology that confounds law enforcement officers. It can also be the legal mechanisms that are shifting or not keeping pace with technology in the first place. Some officers explicitly want to see changes made to the legal mechanisms so that they can be more effective in their job.
Changes to legal mechanisms in order to investigate and prosecute cases

“Faster response to legal paperwork from ISP or providers of internet services: kik...instagram...”

“I feel that web sources allowing this to take place on their sites should be responsible and held accountable. Child pornography is out of control due to a lack of control of webpages.”

“Case history on what is needed for court cases to succeed.”

Although law enforcement officers often feel as though they lack resources, some do identify ongoing efforts to increase communication and share best practices as one of the positive factors shaping how they are working to address the issues at play. In asking respondents how they work to share information, we heard numerous different paths, indicating that some agencies actively share information while others rely on external infrastructure or interpersonal contacts.

Mechanisms for Collaboration and Information Sharing

“I ask fellow investigators via email, chat, or phone conversations. Meetings at conferences and courses.”

“ICAC ListServe, LEIN networks, Training Conferences, Webinars etc.”

“Network with other agencies and ensure that the proper procedures are being taken.”

“By meeting regularly, training technical agents and attending conferences the best practices for the many different judicial districts are distributed. The prosecutors and ICAC supervisors are also vital focal points for knowledge sharing.”

“The latest practices and trends are shared well between ICAC Task Force members. Unfortunately units that are not part of a Task Force are lacking behind in the sharing of this information.”

“We get monthly bulletins consisting of case studies and technological resources from our local internet crimes against children task force.”

“Having a state-by-state listing of investigators, task forces, units that can provide assistance in cross jurisdictional incidents.”

In articulating the resources that they need, law enforcement officers make clear that they see organizational, legal, and technical barriers to move forward. Rather than seeing widely accessible technology as providing them with resources, they see it as requiring new resources that they feel are inaccessible. Although they are working to communicate across agencies and appreciate the collaborative nature of many of their colleagues, they are more worried about issues that they feel are not in their control.
Conclusions

When addressing technology’s role in child sex trafficking crimes, investigators were able to highlight both benefits and obstacles. Benefits included the availability of digital evidence instead of relying on personal accounts, monitoring capabilities of police, and the ability to conduct extensive undercover operations. Obstacles tended to focus on financial and resource concerns, the continual need for training and technical assistance, and the rapidly changing technological environment.

Although child sex trafficking is not a new crime, technology may be providing offenders with some opportunities that were not previously available to them, including access to a wider pool of potential clients, more marketing opportunities, and more avenues for communication with clients and victims. Investigators often feel overwhelmed or ill prepared to handle these shifts.

Technology, for all of its potential, feels more destabilizing than solidifying. And that can be quite daunting when law enforcement officers do not feel as though they have a lot of control over the work that they are trying to do. The political desire is often to get back to the status quo that they know rather than develop new mechanisms for dealing with a changing world. But, in fact, we need law enforcement to be better prepared to deal with the changing world. With that in mind, there are questions of how law enforcement can be empowered to evolve alongside the evolving world around them.

Recommendations

1. Continual education and training for law enforcement is critical in order to stay current with the changing technological environment. This will require both specialization and generalization within and between agencies; organizational structures need to be put into place for this to be more effectively utilized.

2. Collaboration and information sharing may be a critical piece for investigative success. Encouraging communication and information sharing between agencies and between law enforcement, prosecutors, and technical providers could help target these criminals and successfully prosecute them. For example, a centralized database of technology-involved child sex trafficking case characteristics could prove useful from an information-sharing viewpoint.

3. A training manual for various successful investigative techniques would be a useful tool. A process for routine updates as technology evolves would need to be integrated into its development. Perhaps a secure website where investigators could post commentary and ideas about specific techniques could be developed; commentary would need to periodically be examined and key advances could be directly integrated into the manual.

4. More evidence-based research about how often, to what degree, and in what circumstances technology is involved in these crimes would provide a useful perspective within the larger crimes against children investigative field.

5. A financial audit to figure out how to more effectively distribute resources to this space may be called for.
About the Crimes against Children Research Center
The mission of the Crimes against Children Research Center (CCRC) is to combat crimes against children by providing high quality research and statistics to the public, policy makers, law enforcement personnel, and other child welfare practitioners. CCRC is concerned with research about the nature of crimes including child abduction, homicide, rape, assault, and physical and sexual abuse as well as their impact.

The Crimes against Children Research Center proposes four primary goals to comprise a comprehensive and feasible policy for child victims within the criminal justice system.

- Greater recognition of the extent of victimization among the children who come within the purview of the justice system by improved history taking, assessment, record keeping, and exchange of information
- Enhanced protection of child crime victims from continued victimization and from unnecessary trauma and discomfort associated with the workings of the justice system
- Universal rehabilitation of child crime victims through services and programs to aid in recovery and minimize long term effects on development
- Greater public accountability by evaluating the impact of the justice system's policies and programs on children

The Crimes against Children Research Center was created in 1998 at the University of New Hampshire. It grew out of and expands upon the work of the Family Research Laboratory, which has been devoted to the study of family violence and related topics since 1975. Associated with the Center is an internationally recognized group of experts who have published numerous books and articles concerning the incidence and impact of violence against children. CCRC staff have contributed to many pioneering national crime studies, including:

- National Incidence Study of Missing, Abducted, Runaway, and Thrownaway Children
- National Family Violence Survey
- National Youth Victimization Prevention Survey
- National Survey of Sexual Abuse in Day Care
- Developmental Victimization Survey
- Youth Internet Safety Surveys
- The National Survey of Children's Exposure to Violence
- Multi-Site Evaluation of Children's Advocacy Centers
- National Juvenile Online Victimization Studies

Initial funding for the CCRC was provided by the US Department of Justice, Office of Juvenile Justice and Delinquency Prevention. The Center also draws on funding from grants, individual gifts, revenues from publications and programs, and state and federal sources. The CCRC is directed by David Finkelhor, who is also the Co-director of the Family Research Laboratory and Professor of Sociology at the University of New Hampshire. Dr. Finkelhor has been researching criminal violence against children since 1978 and is the author and editor of 10 books and more than 100 articles on the subject.

For more information about Technology-Facilitated Child Sex Trafficking, visit: www.unh.edu/ccrc
References

3. Lantonero M. Human trafficking online: The role of social networking sites and online classifieds. University of Southern California: Annenberg School for Communication and Journalism;2011.
Acknowledgements

We would like to thank Microsoft Research for providing the funding to support this work and for the thoughtful support of Rane Johnson-Stempson and Samantha Doerr in particular. We would also like to acknowledge continual work of colleagues, like Janis Wolak and David Finkelhor, and all the dedicated law enforcement professionals who make it part of their life work to help protect children.