Center for Technology Innovation at BROOKINGS

May 2016

Sextortion: Cybersecurity, teenagers, and remote sexual assault[1]

By Benjamin Wittes, Cody Poplin, Quinta Jurecic & Clara Spera

Benjamin Wittes is a senior fellow in Governance Studies at The Brookings Institution and co-founded and the editor-in-chief of the Lawfare blog

Cody Poplin is a research assistant in Governance Studies at the Brookings Institution and a managing editor of the Lawfare blog.

Quinta Jurecic is a contributor to the Lawfare blog.

Clara Spera is a contributor to the Lawfare blog.

INTRODUCTION

It started with an email from an unknown sender with the subject line, "Read this and be smart."[2]

When the victim opened the email, she found sexually explicit photos of herself attached and information that detailed where she worked. Following that were details of her personal life: her husband and her three kids. And there was a demand.

The demand made this hack different: This computer intrusion was not about money. The perpetrator wanted a pornographic video of the victim. And if she did not send it within one day, he threatened to publish the images already in his possession, and "let [her] family know about [her] dark side." If she contacted law enforcement, he promised he would publish the photos on the Internet too.

Later in the day, to underscore his seriousness, the hacker followed up with another email threatening the victim: "You have six hours."[3]

This victim knew her correspondent only as yosoylammer@hotmail.com, but the attacker turned out to be a talented 32-year-old proficient in multiple computer languages. Located in Santa Ana, California, his name was Luis Mijangos.[4]

On November 5, 2009, yosolammer@hotmail.com sent an email to another woman with the subject line: "who hacked your account READ it!!!"[5] In the email, Mijangos attached a naked photo of the victim and told her "im [sic] in control of your computers right now."[6]

Mijangos had other identities too: Some emails came from christ@yahoo.com; sometimes he was zapotin@hotmail.com.[7] According to court records in his federal criminal prosecution, Mijangos used at least 30 different screen names to avoid detection.[8] But all emails came from the same IP address in Santa Ana.

Law enforcement authorities investigating the emails soon realized that the threatening communications were part of a larger series of crimes. Mijangos, they discovered, had tricked scores of women and teenage girls into downloading malware onto their computers. The malicious software he employed provided access to all files, photos, and videos on the infected computers.[9] It allowed him to see everything typed on their keyboards.[10] And it allowed him to, at will, turn on any web camera and microphone attached to the computer, a capability he used to watch, listen, and record his victims without their knowledge.[11] He kept detailed files on many of his victims, at times gathering information for more than a month, and filling his files with information he could later use to manipulate his victims.[12] Mijangos used a keylogger – a tool that allowed him to see everything typed on a computer – to track whether the victims told friends and family or law enforcement about his scheme.[13] And if they did, he would then threaten them further, notifying them that he knew they had told someone. The malware Mijangos wrote was sophisticated, and he told federal authorities that he designed it specifically to be undetectable to antivirus programs.[14]

In some cases, he tricked victims into creating pornographic images and videos by assuming the online identity of the victims' boyfriends.[15] He then, according to court documents, "used [those] intimate images or videos of female victims he stole or captured to 'sextort' those victims, threatening to post those images or videos on the Internet unless the victims provided more."[16]

Mijangos's threats were not idle. In at least one case, he posted nude photos of a victim on the Myspace account of a friend of the victim, which Mijangos had also hacked, after she refused to comply with his demands.[17]

To make matters worse, Mijangos also used the computers he controlled to spread his malware further, propagating to the people in his victims' address books instant messages that appeared to come from friends and thereby inducing new victims to download his malware.[18]

In all, federal investigators found more than 15,000 webcam-video captures, 900 audio recordings, and 13,000 screen captures on his computers.[19] Mijangos possessed files associated with 129 computers and roughly 230 people.[20] Of those, 44 of his victims were determined to be minors.[21] His scheme reached as far away as New Zealand. The videos he surreptitiously recorded showed victims in various states of undress, getting out of the shower, and having sex with partners.[22] In addition to the intimate material he seized from victims' computers, federal authorities also found credit card and other online account information consistent with identity theft.[23] He sometimes passed this information along to co-conspirators around the world.[24]

Mijangos' actions constitute serial online sexual abuse—something, we shall argue, akin to virtual sexual assault. As the prosecutor said in the case, Mijangos "play[ed] psychological games with his victims"[25] and "some of his victims thoroughly feared him and continued to be traumatized by his criminal conduct."[26] One victim reported feeling "terrorized" by Mijangos, saying that she did not leave her dorm room for a week after the episode.[27] His victims reported signs of immense psychological stress, noting that they had "trouble concentrating, appetite change, increased school and family stress, lack of trust in others, and a desire to be alone."[28] At least one harbored a continuing fear that her attacker would "return."[29]

Mijangos was arrested by the FBI in June 2010.[30] He pled guilty to one count of computer hacking and one count of wiretapping.[31]

He was sentenced to six years imprisonment and is scheduled to be released next year.[32]

* * *

As bizarre as the Mijangos case may sound, his conduct turns out to be not all that unusual. We searched dockets and news stories for criminal cases in which one person used a computer network to extort another into producing pornography or engaging in sexual activity. We found nearly 80 such cases involving, by conservative estimates, more than 3,000 victims.

This is surely the tip of a very large iceberg. Prosecutors colloquially call this sort of crime "sextortion." And while not all cases are as sophisticated as this one, a great many sextortion cases have taken place—in federal courts, in state courts, and internationally—over a relatively short span of time. Each involves an attacker who effectively invades the homes of sometimes large numbers of remote victims and demands the production of sexual activity from them. Sextortion cases involve what are effectively online, remote sexual assaults, sometimes over great distances, sometimes even crossing international borders, and sometimes—as with Mijangos—involving a great many victims.

We tend think of cybersecurity as a problem for governments, major corporations, and—at an individual level—for people with credit card numbers or identities to steal. The average teenage or young-adult Internet user, however, is the very softest of cyber-security targets. Teenagers and young adults don't use strong passwords or two-step verification, as a general rule. They often "sext" one another. They sometimes record pornographic or semi-pornographic images or videos of themselves. And they share material with other teenagers whose cyberdefense practices are even laxer than their own. Sextortion thus turns out to be quite easy to accomplish in a target-rich environment that often does not require more than malicious guile.

For the first time in the history of the world, the global connectivity of the Internet means that you don't have to be in the same country as someone to sexually menace that person.

It is a great mistake, however, to confuse sextortion with consensual sexting or other online teenage flirtations. It is a crime of often unspeakable brutality.

It is also a crime that, as we shall show, does not currently exist in either federal law or the laws of the states. As defined in the Mijangos court documents, sextortion is "a form of extortion and/or blackmail" wherein "the item or service requested/demanded is the performance of a sexual act."[33] The crime takes a number of different forms, and it gets prosecuted under a number of different statutes. Sometimes it involves hacking people's computers to acquire images then used to extort more. More often, it involves manipulation and trickery on social media. But at the core of the crime always lies the intersection of cybersecurity and sexual coercion. For the first time in the history of the world, the global connectivity of the Internet means that you don't have to be in the same country as someone to sexually menace that person.

The problem of this new sex crime of the digital age, fueled by ubiquitous Internet connections and webcams, is almost entirely unstudied. Law enforcement authorities are well aware of it. Brock Nicholson, head of Homeland Security Investigations in Atlanta, Georgia, recently said of online sextoriton, "Predators used to stalk playgrounds. This is the new playground."[34]

But while the FBI has issued numerous warnings about sextortion, the government publishes no data on the subject. Unlike its close cousin, the form of nonconsensual pornography known as "revenge porn," the problem of sextortion has not received sustained press attention or action in numerous state legislatures, in part because with few exceptions, sextortion victims have chosen to remain anonymous, as the law in most jurisdictions permits.

But don't let the problem's invisibility fool you. The 78 cases we reviewed alone involve at least 1,397 victims, and this is undoubtedly just the tip of the iceberg. If the prosecutorial estimates in the various cases are to be believed, the number of actual victims probably ranges between 3,000 and 6,500—and, for reasons we explain below, may be much higher even than that. As the teenage child of one of the present authors put the matter, "You just can't put a portable porn studio in the hands of every teenager in the country and not expect bad things to happen."[35]

This paper represents an effort—to our knowledge the first—to study in depth and across jurisdictions the problems of sextortion. In it, we look at the methods used by perpetrators and the prosecutorial tools authorities have used to bring offenders to justice. We hope that by highlighting the scale and scope of the problem, and the brutality of these cases for the many victims they affect, to spur a close look at both state and federal laws under which these cases get prosecuted.

Our key findings include:

- Sextortion is dramatically understudied. While it's an acknowledged problem both within law enforcement and among private advocates, no government agency publishes data on its prevalence; no private advocacy group does either. The subject lacks an academic literature. Aside from a few prosecutors and investigators who have devoted significant energy to the problem over time, and a few journalists who have written—often excellently—about individual cases, the problem has been largely ignored.

- Yet sextortion is surprisingly common. We identified 78 cases that met our definition of the crime—and a larger number that contained significant elements of the crime but that, for one reason or another, did not fully satisfy our criteria. These cases were prosecuted in 29 states and territories of the United States and three foreign jurisdictions.

- Sextortionists, like other perpetrators of sex crimes, tend to be prolific repeat players. Among the cases we studied, authorities identified at least 10 victims in 25 cases. In 13 cases, moreover, there were at least 20 identified victims. And in four cases, investigators identified more than 100 victims. The numbers get far worse if you consider prosecutorial estimates of the number of additional victims in each case, rather than the number of specifically identified victims. In 13 cases, prosecutors estimated that there were more than 100 victims; in two, prosecutors estimated that there had been "hundreds, if not thousands" of victims.

- Sextortion perpetrators are, in the cases we have seen, uniformly male. Victims, by contrast, vary. Virtually all of the adult victims in these cases are female, and adult sextortion therefore appears to be a species of violence against women. On the other hand, most sextortion victims in this sample are children, and a sizable percentage of the child victims turn out to be boys.

- There is no consistency in the prosecution of sextortion cases. Because no crime of sextortion exists, the cases proceed under a hodgepodge of state and federal laws. Some are prosecuted as child pornography cases. Some

are prosecuted as hacking cases. Some are prosecuted as extortions. Some are prosecuted as stalkings. Conduct that seems remarkably similar to an outside observer produces actions under the most dimly-related of statutes.

Sextortion is brutal. This is not a matter of playful consensual sexting—a subject that has received ample attention from a shocked press.

- These cases thus also produce wild, and in in our judgment indefensible, disparities in sentencing. Many sextortionists, particularly those who prey on minors, receive lengthy sentences under child pornography laws. On the other hand, others—like Mijangos—receive sentences dramatically lighter than they would get for multiple physical attacks on even a fraction of the number of people they are accused of victimizing. In our sample, one perpetrator received only three years in prison for victimizing up to 22 young boys.[36] Another received only 30 months for a case in which federal prosecutors identified 15 separate victims.[37]

- Sentencing is particularly light in one of two key circumstances: (1) when all victims are adults and federal prosecutors thus do not have recourse to the child pornography statutes, or (2) in cases prosecuted at the state level.

- Sextortion is brutal. This is not a matter of playful consensual sexting—a subject that has received ample attention from a shocked press. Sextortion, rather, is a form of sexual exploitation, coercion, and violence, often but not always of children. In many cases, the perpetrators seem to take pleasure in their victims' pleading and protestations that they are scared and underage. In multiple cases we have reviewed, victims contemplate, threaten, or even attempt suicide—sometimes to the apparent pleasure of their tormentors.[38] At least two cases involve either a father or stepfather tormenting children living in his house.[39] Some of the victims are very young. And the impacts on victims can be severe and likely lasting. Many cases result, after all, in images permanently on the Internet on multiple child pornography sites following extended periods of coercion.

- Certain jurisdictions have seen a disproportionate number of sextortion cases. This almost certainly reflects devoted investigators and prosecutors in those locales, and not a higher incidence of the offense. Rather, our data suggest that sextortion is taking place anywhere social media penetration is ubiquitous.

The paper proceeds in several distinct parts. We begin with a literature review of the limited existing scholarship and data on sextortion. We then outline our methodology for collecting and analyzing data for the present study. We then offer a working definition of sextortion. In the subsequent section, we provide a sketch of the aggregate statistics revealed by our data concerning the scope of the sextortion problem, and we examine the statutes used and sentences delivered in federal and state sextortion cases. We then turn to detailing several specific case studies in sextortion. In our last empirical section, we look briefly at the victim impact of these crimes. Finally, we offer several recommendations for policymakers, law enforcement, parents, teachers, and victims.

We offer more detailed legislative recommendations in a separate paper, "Closing the Sextortion Sentencing Gap: A Legislative Proposal."[40]

AN UNDERSTUDIED PROBLEM

Sextortion is remarkably understudied. Despite the rash of sextortion cases, some of them reasonably prominent, press attention to the issue has been modest, particularly in comparison to the dramatic attention devoted to issues of online bullying, child pornography generally, and revenge porn. While federal law enforcement has responded vigorously to individual cases around the country, a broader policy discussion has not followed. Most people, we suspect, have never heard of sextortion.

The term "sextortion" is not new. It began popping up in news coverage of incidents of sexual extortion involving online sexual exchanges with relative frequency beginning in 2010,[41] though we found one use of the term dating back to 1950.[42] Prosecutors use the term routinely in public statements to describe a certain type of case.[43]

Still, there has been no serious academic research surrounding sextortion. There have been no studies examining the most basic questions surrounding the problem: How common are these cases? What are the basic elements that characterize them? Are our laws adequate for the investigation and prosecution of sextortion cases?

After this text of this paper was finalized for publication, the U.S. Department of Justice released "The National Strategy for Child Exploitation Prevention and Interdiction," a report to Congress. Released on April 19, 2016, that document discusses in greater depth than the department had in the past the crime of sextortion, at least as committed against children, and is consistent with the findings published in this report that relate to child sexual exploitation. The Justice Department report confirms that "sextortion is by far the most significantly growing threat to children" and that "sextortion cases tend to have more minor victims per offender than all other child sexual exploitation offenses." The document also references a 2015 FBI analysis of 43 cases of sextortion which found that "at least 28 percent of these cases had at least one victim who committed or attempted suicide." As of this writing, however, the FBI has not made this analysis available to us. The National Strategy is a recommended resource for anyone looking to gather information as to how law enforcement plans to tackle the growing crime of sextortion. It suffers, however, from several of the deficiencies on which we have focused in this report. It contains no authoritative data on the scope of the problem or on the number of prosecutions. And the document focuses exclusively on the problem of sextortion as a species of child exploitation, ignoring the many adults victimized as well.

Citation: U.S. Dep't of Justice, The National Strategy for Child Exploitation Prevention and Interdiction, (April 2016), https://www.justice.gov/psc/file/842411/download.

For its part, the press has tended to report on individual cases, not on the phenomenon more broadly. Mentions of the larger problem tend to be passing ones. The *New York Times*, for example, recently ran a short piece in its "Sunday Review" section, outlining all types of scams that those looking for love on the Internet might encounter, including sextortion.[44] Another *Times* article on the anonymous messaging app Kik noted that law enforcement commonly comes across the app in connection with sextortion cases.[45] In these *Times* pieces, as with most instances, the mention of sextortion is fleeting.

GQ magazine has run two feature-length stories on sextortion, both focused on individual cases. In 2009, the magazine covered the story of Anthony Stancl, a troubled and bullied student at New Berlin Eisenhower high school in Wisconsin, who tricked fellow male students into sending

him sexually explicit photos and videos as both a form of sexual gratification and also social revenge.[46] Though the title of the *GQ* piece about Stancl references sextortion, the piece does not explore the subject beyond Stancl's own case.

In 2011, *GQ* readers also learned of Mijangos in an article that does highlight the unique qualities of sextortion. That article explained that "[d]espite billions spent on technology that lets us broadcast our daily lives, all it takes is one guy, a self-taught hacker with no college degree, to turn that power against us."[47] A number of media outlets have done brief pieces on the problem.[48]

The Justice Department's in-house bulletin for prosecutors has specifically addressed the sextortion phenomenon only once, in 2011.

The Digital Citizens Alliance touched on sextortion tangentially as part of a report on remote access trojans (RATs). The report, among other things, demonstrated that RATs like the one used by Mijangos are easily accessible and quite affordable. On one hacker website, the authors found an advertisement for access to computers that belong to girls for $5 each; access to a boy's computer sold for less, only $1 each. The report also notes thousands of tutorials on YouTube, instructing hackers on the best techniques for slaving a device; other videos appear to show off an individual hacker's exploits, displaying videos of victims from their own webcams. Yet this report, published in 2015, focused on the cybersecurity problem of RATs broadly, and less on the exploitations at play in sextortion cases.[49]

Government attention has likewise been spotty. The Justice Department's in-house bulletin for prosecutors has specifically addressed the sextortion phenomenon only once, in 2011, and then in a brief, five-page article on charging options for cases involving underage victims only.[50] The Federal Bureau of Investigation cautioned parents and their children about the sextortion threat in a 2012 advisory.[51] The following year, the Bureau's then-director touched on sextortion in a stray paragraph in congressional testimony that canvassed the Bureau's various law enforcement and other activities.[52] In 2015, the FBI once again warned parents and children following the conviction of one Lucas Michael Chansler (see case studies below), this time calling on the public for more information about Chansler's crimes,[53] and releasing a video explaining how sextortion occurs and how parents should talk to their children about it.[54] As part of the same release, the FBI also produced a short, one-minute radio briefing on the "growing number of reports of sextortion."[55] A separate sextortion fact sheet, released at the same time, provided more information on how perpetrators carry out their crimes, and ways for parents and children to protect themselves from those who would try to sextort them.[56]

Yet there has never been a congressional hearing on sextortion as a free-standing issue, and neither current nor proposed legislation so much as mentions the phenomenon. To the extent sextortion is on officialdom's radar at all, it appears only as part and parcel of a bigger struggle to beat back online sex offenses more generally.

The scholarship has trended along similar lines. Some legal scholarship has alluded to sextortion, but only in passing.[57] Legal academics have noted the phenomenon in the context of computer crimes more broadly, but have not concentrated on sextortion as a focus of study.

Take for example Dayton Law Professor Susan Brenner's book "Cybercrime and the Law," which dedicated only four of its 219 pages to the crime of sextortion. After noting that cyber sexual extortion is a new but rising phenomenon and naming a few recent cases, Brenner concludes that extortion statutes wherein the target's property is presumed

to have value in the "traditional, financial sense" may present difficulties for prosecutors in these cases. She suggests prosecutors may be successful by "(1) adopting new, sextortion-specific statutes or (2) revising existing extortion statutes so they encompass the type of harm inflicted in sextortion cases."[58] Danielle Keats Citron's excellent book, "Hate Crimes in Cyberspace," contains extensive discussion of revenge porn and virtually no discussion of sextortion.[59]

Nor are data, either official or private, readily available. We sought data on sextortion cases from the Bureau of Justice Statistics, which informed us that they "are not able to separate out" sextortion cases from other types of cases, as "federal data is based on statute and does not provide the detail needed to identify these offenses."[60] We also sought data from the FBI; despite the Bureau's warnings on the subject, it could provide only a link to a webpage describing the Bureau's Violent Crimes Against Children (VCAC) program.[61] The Department of Justice was able to flag eight specific sextortion cases but noted that this was a "sampling" because "the department does not have a data-tracking category for sextortion."[62]

We also sought data from activist organizations aware of and concerned about the problem. We contacted the Cyber Civil Rights Initiative,[63] the Cyber Civil Rights Legal Project,[64] the Family Online Safety Institute,[65] Thorn,[66] and the National Center for Missing and Exploited Children (NCMEC),[67] none of which could provide data on the prevalence of sextortion cases nationally. The NCMEC has published a limited set of data culled from its CyberTipline, which it reports in part as follows:

- 78 percent of the incidents involved female children and 12 percent involved male children (In 10 percent of incidents, child gender could not be determined);
- The average age at the time of the incident was approximately 15 years old, despite a wider age-range for female children (eight-17 years old) compared to male children (11-17 years old); and
- In 22 percent of the reports, the reporter mentioned being suspicious of, or knowing that, multiple children were targeted by the same offender.

…

Based on the information known by the CyberTipline reporter, sextortion appears to have occurred with one of three primary objectives (In 12 percent of reports, the objective could not be determined):

- To acquire additional, and often increasingly more explicit, sexual content (photos/videos) of the child (76 percent)
- To obtain money from the child (six percent)
- To have sex with the child (six percent)

…

Sextortion most commonly occurred via phone/tablet messaging apps, social networking sites, and during video chats.

- In 41 percent of reports, it was suspected or known that multiple online platforms were involved in facilitating communication between the offender and child. These reports seemed to indicate a pattern whereby the offender would intentionally and systematically move the communication with the child from one online platform type to another.

- Commonly, the offender would approach the child on a social networking site and then attempt to move the communication to anonymous messaging apps or video chats where he/she would obtain sexually explicit content from the child. The child would then be threatened to have this content posted online, particularly on social media sites where their family and friends would see, if the child did not do what the offender wanted.[68]

These data, though useful and illuminating and broadly consistent with our own findings, are necessarily limited. Because they are only based on victim reporting, there is no information about subsequent prosecutions, investigative findings, or critically, victims *other than ones who initially reported the offenses*. That turns out to be a fateful omission.

Our point is not to criticize any of these organizations, or government agencies, for the lack of data on the subject. The problem of sextortion is, in fact, new. It remains relatively undefined. And at least with respect to the activist groups, it is a perfectly reasonable approach to focus on revenge porn first and on the problem of non-consensual pornography—of which sextortion is just one species—more generally. The result, however, is a certain gap in our understanding of this new form of crime. How big a problem is it really? How many people does it affect? And how should we define it? This paper represents a systematic effort to examine these problems.

METHODS

Because of the disaggregated nature of the data we sought, the breadth of the problem, and the numerous criminal statutes available for possible prosecutorial use, we began with a systematic search of media on sextortion. Using LexisNexis, we searched media databases in all 50 states and the District of Columbia for keywords related to sextortion. We used the following keywords: “Sextort,” “Sextortion,” “Cyber Sextortion,” “Cyber Sexual Extortion,” “Cyber Sexual Exploitation,” “Online Sexual Extortion,” “Online Sexual Exploitation,” “Non-consensual Pornography,” and “Nonconsensual Pornography.” Using the same keywords, we then also searched WestLaw, looking for legal opinions involving sextortion.

We then read all media results that our searches of LexisNexis returned, selecting those cases from articles that fit the parameters we set for sextortion cases (described below). We identified 78 cases, 63 of them federal from 39 different judicial districts, 12 of them from the state courts of eight states, and three of them international cases from Israel, Mexico, and the Netherlands. In some instances, prosecutors we contacted made us aware of other cases. In other instances, the cases themselves cited earlier sextortion cases. As we progressed, a number of news stories made us aware of additional cases that arose after our searches took place.

For federal cases, we used both the Public Access to Court Electronic Records (PACER) service and proprietary online databases to gather the warrant applications, complaints, indictments, plea agreements, and judgments for the individual cases, as available, as well as other relevant documents that describe the conduct at issue in the cases.

For state and international cases, we acquired original court documents where possible, but both for language and document-availability reasons, we also relied to a considerable degree on press accounts.

We examined each case to discern the number of clearly-identified (generally not by name) victims, the maximum number of victims estimated by prosecutors, the ages and genders of the victims, the number of states and countries involved in the offense pattern, and the sentence given the defendant (if any). We also tracked certain common elements of sextortion cases, both those charged and those pled or convicted; specifically, we identified the following recurrent elements in all cases in which they arose:

- computer hacking;
- manipulation of victims using social media (catfishing);
- interstate victimization;
- international victimization; and
- demand for in-person sexual activity.

For those cases prosecuted federally, we also looked specifically at the criminal offenses charged in each case, as well as those to which the defendant either pled guilty or was convicted.

The data we report here reflect our best sense of the sextortion landscape as of April 18, 2016. This report reflects neither developments within cases after that date nor new cases that have arisen since that date.

We are confident that this dataset is not complete. That is, there are sextortion cases both domestically and overseas, probably many of them, that we have not identified. We are even more confident that an enormous number of victims have not reported acts that would warrant aggressive investigation and prosecution along the lines of the cases we have found. We have identified the cases discussed in this study, in other words, not as illustrating the totality of the sextortion problem but as a significant and illustrative sample of it. We do not purport to know if it represents the bulk of the cases that have been prosecuted or not. We believe, however, that the prosecuted cases, like other forms of sexual assault, likely reflect a tiny percentage of the unprosecuted ones, meaning that we should understand online sextortion as a feature of life on the Internet for large numbers of vulnerable members of society.

Finally, one additional methodological note: For purposes of this study, we have taken prosecutorial allegations in many instances as true. Each of these cases involves an adjudication, and defendants are entitled to a presumption of innocence in the absence of proof beyond a reasonable doubt. We are not, however, an adjudicative body. We are, rather, looking to understand empirically the scope and depth of a social problem. As such, conduct that the FBI or prosecutors believe has taken place but for which a defendant has not been convicted may be just as interesting as that conduct which has generated a conviction. This point is especially important with respect to estimates as to the number of victims in different cases and to conduct charged but dropped in the context of plea agreements.

A WORKING DEFINITION OF SEXTORTION

Legally speaking, there's no such thing as sextortion. The word is a kind a prosecutorial slang for a class of obviously criminal conduct that does not in reality correspond neatly with any known criminal offense. Sextortion cases are sometimes prosecuted under child pornography laws, sometimes as computer intrusions, sometimes as stalkings,

and sometimes as extortions. The term "sextortion" lacks a precise definition of its own, much less clear elements of the sort that arise out of legislative definition.

Still, at a high level of altitude, the conduct is easy enough to describe: **sextortion is old-fashioned extortion or blackmail, carried out over a computer network, involving some threat—generally but not always a threat to release sexually-explicit images of the victim—if the victim does not engage in some form of further sexual activity.**

> Every single perpetrator in the cases we examined is male.

By defining sextortion in this fashion, it is important to understand that we are excluding a variety of closely-related coercive activities that may also warrant more attention than they have received. For example, it is possible for something like sextortion to take place entirely offline; indeed, sexual extortion has taken place as long as people have had the power to demand sex from one another on threat of doing each other harm. We have not included any cases where conduct takes place solely in the offline world, however, on the theory both that this is an old problem that the law has had many generations to address and that it does not pose the same inter-jurisdictional and cyber-security problems as do the same activities online. When we say "sextortion," therefore, we are talking only about *online sexual extortion*. None of this is to diminish the horrifying extortions by which, for example, many pimps keep women in forms of sexual slavery.

Similarly, in the course of our research, we have discovered a number of cases—including several celebrated "revenge porn" cases—that have significant elements of sextortion and in which the threat of exposure of sexually-explicit material is used to extort money, but in which sexual activity itself is not demanded of the victim.[69] In online sexually-oriented extortion, it is possible for a perpetrator to use the release of sexual images or videos as a threat against the victim; the production of sexual images or videos can also be the demand; most commonly, both take place at once. That is, the perpetrator uses the threat of the release of material to coerce the production of more material.

A related but distinct problem is that of online scams that extort *money* from individuals after they have engaged in anonymous online sexual video chatting—for example over Skype. One such syndicate in the Philippines was busted in 2015. Following a tip, Philippine police arrested 58 people and seized 250 computers in seven areas across the country. Police said the extortionists acquired hundreds of victims in Australia, Singapore, Hong Kong, the United States, and the United Kingdom over the course of three to four years. The group found and friended victims over various social media sites, inviting them to engage in cybersex. After surreptitiously filming the chats, the group would then demand up to $2,000 in exchange for not publicly posting the material. The national police chief of the Philippines compared the group to a call center, where employees sit in rows of cubicles luring in foreign victims. The extortion ring was broken up only after its activity led to the suicide of one 17-year-old boy located in Scotland.[70]

While these cases, and others like them, can be extremely severe and present their own cybersecurity and privacy problems, *we have excluded from this analysis all cases in which sexual activity was not demanded of the victim.* If a perpetrator threatens a victim with exposure of sexually-explicit videos unless she pays him money, we have not included that in our sample unless the perpetrator also demands the production of further sexual images or videos.

A majority of the cases we examined overtly crossed state lines, sometimes the lines of many states.

The reason for this decision is that the primary phenomenon we seek to define here is the remote coercion of sex. The remote coercion of money using sexual images is not a new problem, though the Internet has certainly made it worse. The ability of a person to force someone halfway around the world to engage in sexual activity, by contrast, is a new form of digital abuse that was unthinkable only a few years ago. The ability of a single perpetrator to exploit hundreds, or even thousands, of victims around the world was particularly beyond our collective imaginations.

We have thus proposed a relatively narrow definition that excludes a considerable body of related criminal activity in an effort to focus attention on what is new here.

THE DATA IN AGGREGATE

We have included in this analysis a total of 78 cases[71] in 52 different jurisdictions,[72] 29 states or territories,[73] and three foreign countries.

Fifty-five of those cases (71 percent) involve only minor victims.[74] An additional 14 (18 percent), by contrast, involve a mix of minor victims and adult victims.[75] In nine cases (12 percent), all identified victims were adults.[76]

Every single perpetrator in the cases we examined is male. The vast majority of the victims, by contrast, are female. Among the adult victims, nearly all are female.[77] The picture is more complicated among the child victims, where a significant minority of victims is male. In 13 cases (17 percent) involving minor victims, all identified victims in court documents are male.[78] In an additional eight cases (10 percent), the victims include both males and females.[79] Several truly brutal cases focus on young boys. So it's a mistake to think of sextortion as purely a problem of violence against women. There is clearly a problem with respect to boys as well.

The length of a given perpetrator's sentence tends to turn less on the number of victims or the brutality of the conduct involved in the case than on whether the victims are minors or adults. The reason is that federal child pornography laws carry particularly stiff sentences, far stiffer than those at issue with stalking, extortion, or computer intrusion laws. The result is that of those cases that involved minor victims and did not produce a life sentence, the sentencing range varied from seven months to 139 years imprisonment, with a median of 288 months (24 years) and a mean sentence of 369 months (31 years). Cases that involved only adult victims, by contrast, involved sentencing ranges from one month to 6.5 years imprisonment, a median sentence of only 40 months and a mean sentence of 38 months.

By far, the most common feature of sextortion cases is social media manipulation, in which the perpetrator tricks the victim into sending him the compromising pictures he then uses to extort more. Social media manipulation of some kind is present in the overwhelming majority of cases. Fully 65 cases (83 percent) involve some form of social media manipulation.[80] Also known as "catfishing," this behavior is even more common when the victim is a minor, with some form of social media manipulation featuring in 91 percent of the cases involving minors.[81] Only three cases with only adult victims, by contrast, involved catfishing.[82] Alternatively, some form of computer hacking was involved

in 43 percent of cases with adult victims,[83] but only nine percent of cases only involving only minor victims.[84] Hacking featured in 15 cases (19 percent) total.[85]

In many of the cases involving catfishing, the defendant used information he had somehow discovered about the victim to make his catfishing more effective. In one case, the information in question was obtained by hacking the victim's computer.[86] In at least one other case, the defendant looked up information available online.[87] In another, the defendant worked as a camp counselor over the summer and accumulated information about campers over the course of his job—and then later used that info to catfish and blackmail them.[88] Similarly, the criminal complaint in one case alleges that the defendant used personal information he knew about his victims from his offline interactions with them to make his threats more effective.[89]

The same cybersecurity vulnerabilities that are making our corporations and government agencies ripe for cyber exploitations from foreign intelligence agencies and hackers are making teenagers and young adults ripe for highly-remote sexual exploitations.

A majority of the cases we examined overtly crossed state lines, sometimes the lines of many states. Forty nine cases (63 percent) involved significant interstate elements: the perpetrator, for example, victimizing people in other states.[90] At least six cases involved more than ten jurisdictions, either foreign or domestic.[91] Seven additional cases involved more than five jurisdictions.[92]

A surprising number of cases cross international borders as well. Sixteen cases (21 percent) involve a perpetrator victimizing at least one person in a country other than that in which he is himself residing.[93] This finding seems particularly challenging. It used to be impossible to sexually assault someone in a different country. That is no longer true. The same cybersecurity vulnerabilities that are making our corporations and government agencies ripe for cyber exploitations from foreign intelligence agencies and hackers are making teenagers and young adults ripe for highly-remote sexual exploitations.

Some cases manage to leap out of the online world and involve abuse in the physical world. In 13 cases (17 percent) perpetrators demanded actual in-person sexual activity from victims, not merely the production of pornographic materials.[94] This category of case hints at one of the fault lines in sextortion cases. The majority of sextortionists are after targets of opportunity on social media. Some sextortion cases, by contrast, are highly-targeted cases of intimate abuse: a former boyfriend who can't let go and goes after his ex-girlfriend's daughter,[95] a father bent on molesting his daughter,[96] or some other person with a pathological obsession with a particular victim.[97] These cases tend to look more like stalking—and are often prosecuted as such. They tend to involve smaller numbers of victims. But they are also far likelier to involve physical abuse of those victims. In some of these cases, sextortion is only a part of a far larger pattern of abuse.

Calculating the total number of victims in these cases is impossible. The cases cumulatively identify 1,397 victims, but these are only the victims counted by authorities in charging or alleging specific conduct against a particular defendant. For example, if prosecutors included a specific reference to a particular sextortion victim in a charging document, a complaint, or a plea agreement, or if a sentencing memo says that a particular number of victims has been identified, this victim—or this number of victims—will be included in this total figure.

This way of counting, however, grossly undercounts the true number of victims. In many cases, prosecutors do not charge a defendant with every instance of sextortion of which they have reason to believe him guilty; they charge, rather, only conduct related to those victims where the evidence is most developed. Along the way, they sometimes mention a much larger figure of other cases in which they believe the same perpetrator was involved.

The disparities between the number of identified victims and the number estimated can be extreme. For example, in the case of Brian Caputo—a California man accused in federal court of posing as a teenage girl on social media to trick real teenage girls into sending him explicit pictures—prosecutors identified "at least eight possible minor victims." On the other hand, in the same document, they say that they have found 843 emails in which "almost every e-mail either contained child pornography or was [Caputo] communicating with possible other unidentified victims."[98] Similarly, in the particularly sinister case of Richard Leon Finkbiner (detailed below), prosecutors identified only thirteen victims, but they made clear that those victims stood in for "hundreds, if not thousands, of other minors and adults all over the world" whom Finkbiner also sextorted.[99] In some cases, the best prosecutorial estimates of the total number of victims are quite vague. The government frequently describes "numerous" victims, for example; in some cases it refers to "hundreds" or "more than 100" or some such minimum round number. By contrast, in some cases, investigators seem to have gone through a great deal of trouble to identify every victim they could. All of this makes any effort to estimate the total size of the victim population necessarily a back-of-the-envelope sort of calculation.

Still, it is possible in very round terms to give a sense of the magnitude of the victim population. If we take the list of prosecutorial estimates of the likely number of victims in each case, and we make a series of different assumptions about what certain terms suggest on average, we can come up with various estimates.[100]

A conservative approach would be to assume that when prosecutors describe a given sextortionist as having "numerous" victims, "numerous" will work out on average to around 20, that "hundreds" should be interpreted conservatively to mean 100, and that we should take the lowest figure in any range (meaning that a phrase like "between 100 and 150" should mean 100). Tabulated this way, the total victim court comes out to be around 3,200.

A more aggressive approach would be to assume that when prosecutors are only dealing with 20 victims, they tend to identify them and count them, and therefore phrases like "numerous" should mean something more like 50. Similarly, "hundreds" should refer to at least 200, and more than X should refer to something close to 150 percent of X than to X itself. In this approach, we take in any range of numbers the mean between the two poles. The phrase "at least hundreds and possibly thousands," meanwhile, should imply something more like 750 than 100. Using this method of tabulation, the figure works out to be more than 5,200.

Even this approach, however, may involve a substantial undercount. In many cases, prosecutors do not even attempt an accounting of the total number of victims. They merely identify a few victims and prosecute based on those few, leaving the rest uncounted. There are thus a bunch of cases that are clearly not intimate abuse cases—say stalkings of individuals, which are highly targeted at those individuals—but give every indication, rather, of being more indiscriminate. Yet these 28 cases identify, like the intimate abuse cases, only one or two victims and lack a high-end estimate as to the number of victims. We think this is likely not because the number of identified victims is, in fact, equal to the total number of victims but—in most cases—because prosecutors did not bother to include estimates in their pleadings or because investigators did not bother to count other possible victims. To compensate for this, we examined the average disparity between the high-end victim estimate and the number of identified victims in those cases in which a high-end estimate does exist, using the more aggressive assumptions in our second model.

In those cases, the high-end victim estimate averages to 4.6 times the number of identified victims. Using this multiplier for the set of 28, we estimate that a reasonable guess as to the total number of victims may include up to an additional 1,500 people.

Put simply, we think a reasonable estimate of total victims in these cases will run anywhere from about 3,000 to about 6,500.

There's at least one additional complicating factor. A single pair of sextortionists, the FBI has estimated, may have as many as 3,800 victims between them. This estimate does not appear in the court documents associated with their cases, which we discuss below. But the FBI has stated it publicly elsewhere.[101] If that figure is correct, the entire range—calculated by whatever means and with whatever assumptions—needs to be shifted upward by nearly several thousand victims.

PROSECUTING SEXTORTION

One of the most interesting features of sextortion cases is the diversity of statutes under which authorities prosecute them. As we noted above, sextortion does not exist in federal or state law as a crime of its own. So sextortionate patterns of conduct can plausibly implicate any number of criminal statutes, which carry very different penalties and elements.

In the federal system, at least, the workhorse statute is 18 USC § 2251, which prohibits sexual exploitation of children. Prosecutors charged under this law in 43 of the cases under study here (55 percent).[102] In particular, subsection § 2251(a) does a great deal of heavy lifting for prosecutors. Under that section, "Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in . . . any sexually explicit conduct for the purpose of producing any visual depiction of such conduct" is subject to a mandatory minimum sentence of 15 years in prison.[103]

> In other words, absent a child victim, there's no obvious on-point federal law that covers the sexual elements of sextortion.

More generally, the child pornography laws provide powerful tools of choice for prosecutors, at least in the cases in which minor victims are involved. Section § 2252 of Title 18, which relates to materials associated with the sexual exploitation of children, can be used to prosecute both receipt and distribution of child pornography and possession of it; charges under this section show up in 28 cases (36 percent).[104] Seventeen cases (22 percent) also contain charges under the adjacent section § 2252A, which is a parallel law related to child pornography in particular.[105] And 18 USC § 2422(b), which forbids coercion or enticement of a minor to engage in illegal sexual activity, shows up in 19 cases (24 percent).[106] Where they are available, the child pornography laws do clearly give prosecutors the tools they need, owing to the stiff sentences they mete out.

The trouble is that not all sextortionists prey on children, and where none of the victims involved in the conduct charged is a minor, the cases fall into something of a statutory lacuna. After all, without touching someone or issuing a threat of force, it is not possible to violate the aggravated sexual abuse law (18 USC § 2241), which only applies in any event in the special maritime or territorial jurisdiction of the United States or in a prison facility. (That same jurisdictional

limit applies to the lesser crime of sexual abuse, 18 USC § 2242, and other federal sex crimes statutes.) In other words, absent a child victim, there's no obvious on-point federal law that covers the sexual elements of sextortion.

The result is a frequent prosecutorial reliance on the federal interstate extortion statute (18 USC § 875)—the relevant portion of which carries only a two year sentence. This law shows up in 29 of the federal cases we examined (37 percent).

In cases in which the attacks are highly targeted against an individual, prosecutors have sometimes relied on the federal stalking law (18 USC § 2261A), charges under which appear in nine cases (12 percent). And in 12 cases (15 percent) involving hacking or appropriation of social media accounts, prosecutors have used the Computer Fraud and Abuse Act (18 USC § 1030), the identity theft law (18 USC § 1028A), or both.

As we noted above, these cases produce sentences on average dramatically lower than those charged under the child exploitation laws. This is partly because the child pornography laws carry particularly severe sentences, but it's also because sextortion cases end up outside of the arena of sex crimes and prosecuted as hacking and extortion cases. As we argue in "Closing the Sextortion Sentencing Gap," Congress should examine closely the question of whether sextortionists who prey on adults—sometimes many of them—are receiving excessively lenient treatment under current law. Suffice it for present purposes to observe that there is no analog for adult victims to 18 USC § 2422's criminalization of coercing a minor to engage in sexual activity (at least if that sexual activity does not involve prostitution or otherwise illegal activity). And while 18 USC § 875, the extortion statute, permits a 20-year sentence for the transmittal of a ransom demand, and the same stiff term for anyone who transmits a "threat to injure the person of another," the statute offers only a two-year sentence for anyone who, "with intent to extort from any person . . . any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee." It contains no enhanced sentence for the situation in which the thing of value in question being extorted is coerced production of nonconsensual pornography.

Another area in which current law looks deficient is at the state level. State prosecutors are among those who have done the most dedicated work in this area. But the data in aggregate strongly suggest that they are working with weak tools compared to their federal counterparts. The average sentence in the six state cases that have reached the sentencing phases is 88 months (seven years and four months). By contrast, the average sentence in the 49 federal cases that have produced a sentence less than life in prison (one case has produced a life sentence) is, by contrast, 349 months (a little over 29 years).

This dramatic disparity is only partly a reflection of strong federal child pornography sentencing. It also reflects weak state laws that are under-punishing serious offenders. For example, Joseph Simone in Rhode Island, who sextorted 22 teenage boys in a particularly brutal fashion, received only one year in prison and two more years of home confinement (and an additional period of probation).[107] Similarly, it's hard to imagine that had Cameron Wiley been prosecuted in federal court for sextorting two underage girls, he would have received only seven months in jail and an additional 18 months of probation—as he did in Wisconsin state court.[108]

CASE STUDIES IN SEXTORTION

Sextortion cases vary. Most involve relatively simple social media manipulations, in which the perpetrator tricks victims into sending him one or more nude photographs and then uses the threat of release of those photos to

extort the production of larger numbers of more explicit ones. These attacks tend to have large numbers of victims and to be relatively indiscriminate. As noted above, however, some sextortion cases involve highly targeted attacks on individuals known personally to the perpetrator. A smaller number involve one or more forms of hacking, either intrusions into victims' social media accounts or, in some instances, the actual hacking of their computers and the remote controlling of their webcams.

What follows are detailed accounts of eight sextortion cases; the accounts are culled from court documents to give readers a flavor of both the common threads between the cases and the diversity among them. Our goal is both to describe the mechanics of sextortion and to portray how the crime operates on its victims, with the aim of communicating the seriousness of these offenses.

JARED JAMES ABRAHAMS

Jared James Abrahams, a California college freshman studying computer science, was arrested in 2013 for the sextortion of the woman who would become the crime's best-known victim: Cassidy Wolf, that year's winner of the Miss Teen USA beauty pageant.[109] Abrahams and Wolf had gone to high school together in Temecula, California.[110] She first suspected that something was wrong when she received notifications from several social media services that someone had tried to change her passwords. Thirty minutes later, Abrahams emailed her, demanding that she either send him nude pictures of herself on the social media service Snapchat, send a "good quality video," or Skype with him "and do what I tell you to do for five minutes." Otherwise, he would upload naked pictures of her to her social media accounts. Wolf did not recognize the photos, which appeared to have been taken from her webcam.[111]

Investigators later found that Abrahams had sextorted at least 12 young women, including women from Ireland, Canada, and Moldova and controlled the computers of between 100 and 150 women[112] He installed keylogger software on his victims' computers to record their passwords and gain access to their social media accounts—though he mocked Wolf for making her passwords so easy for him to guess.[113] He would also install the malware programs Blackshades and DarkComet, which enabled him to remotely control his victims' webcams without their knowledge and surreptitiously take photographs.[114] He often contacted victims using other email addresses that he had hacked, and would use the productivity software Bananatag and Toutapp to monitor when his victims read his emails.[115]

One victim wrote to Abrahams, "Please remember im only 17. Have a heart." He responded, "I'll tell you this right now! I do NOT have a heart!! However I do stick to my deals! Also age doesn't mean a thing to me!!!"[116]

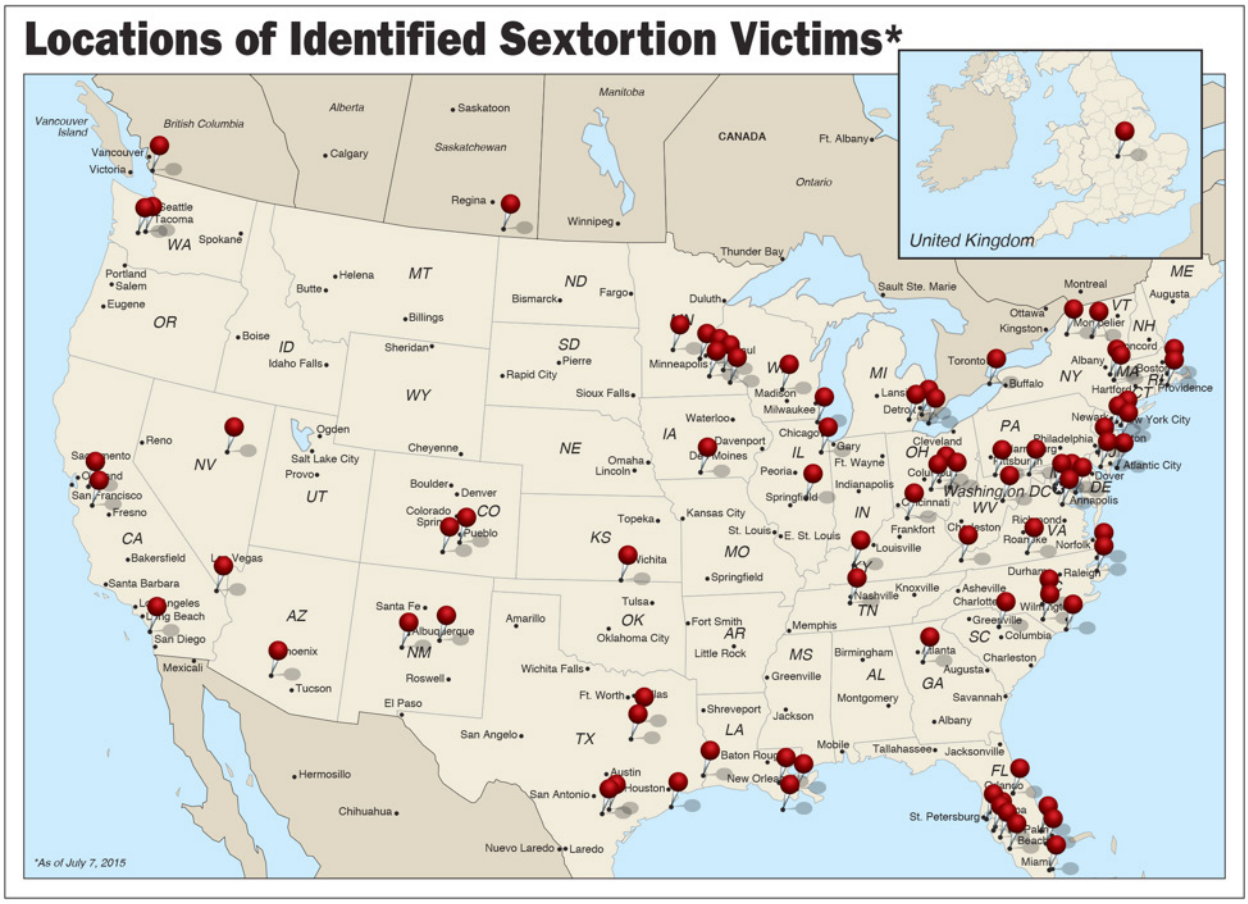
In order to hide his IP address, Abrahams used a Virtual Private Network (VPN) service that advertised it did not keep logs,[117] along with a dynamic DNS service offered by No-IP.com.[118] Investigators ultimately traced the IP address back to Abrahams, discovering that a person with the same username used to register for No-IP.com had also posted on hacking forums bragging that he had infected the computer of someone who "happened to be a model." The username in question? "Cutefuzzypuppy."[119]

Abrahams was charged with one count of computer fraud and three counts of extortion, and pleaded guilty to all charges.[120] He was sentenced to 18 months in prison.[121]

LUCAS MICHAEL CHANSLER

From 2007 to 2010, Lucas Michael Chansler targeted nearly 350 young girls in his sextortion ploy—so many that, after his arrest, the FBI launched a prolonged online campaign to locate the scores of girls whom he had victimized.[122] Agents wanted to interview the girls for information on Chansler's case, but they also wanted to provide closure. After all, there was no other way that victims would know that their torture had been ended for good.[123]

Hiding his IP address through proxy servers, Chansler relied on catfishing to reach out to potential targets through social media.[124] Pretending to be a teenage boy—usually interested in skateboarding—who was looking for a friendship or flirtation with the victim, Chansler would ask to video chat with the victim and display video of a naked boy in order to hide his identity. He asked the victims to strip on camera, and he secretly recorded the stream.[125] In one case, he tricked four young girls at a sleepover into posing for him on Stickam, a now-discontinued livestreaming service notorious for the predatory behavior of some of its users and notorious as well because of its owner, a businessman who also controlled a network of pornographic websites.[126] Once Chansler had the video or pictures that he wanted, he threatened to release the material to the victim's friends and family or upload it to a public website unless the victim provided him with more.[127] In an interview with the FBI, one victim described the depression and panic caused by Chansler's demands that she constantly be available to respond to his messages: "I felt like a slave. . . . I remember just lying in bed in silence and just thinking. I felt like God was so disappointed in me, and I didn't know what to do."[128]



[FBI MAP: https://www.fbi.gov/news/stories/2015/july/sextortion; https://www.fbi.gov/news/stories/2015/july/sextortion/image/map-showing-locations-of-identified-sextortion-victims]

Speaking with an FBI agent after his arrest, Chansler explained that he targeted young girls because they were more likely to believe his scam.[129] He was charged with four counts of extortion, 14 counts of producing child pornography, one count of receiving child pornography, and one count of possessing child pornography.[130] He pleaded guilty to all 14 counts of producing child pornography and has been sentenced to 105 years in federal prison.[131]

IVORY DICKERSON AND PATRICK CONNOLLY

Ivory Dickerson and Patrick Connolly never met in person, but they functioned together as a kind of sextortion team: together, the FBI claims, they targeted more than 3,800 underage girls.[132] Dickerson—a civil engineer in North Carolina—and Connolly—a British military contractor working at a U.S. base in Baghdad—worked in tandem,[133] with Connolly usually reaching out to potential victims over the internet in order to trick them into installing the malware Bifrost.[134] Then the two would collaborate in blackmailing their victims with photos taken surreptitiously using their webcams or with personal information obtained by their computers.[135] It took four years of investigation to track them down.[136]

In one case, Connolly threatened to post a girl's email address online and to harm her younger sister unless she provided photographs.[137] In another, he told a victim that he would make her "the most well-known girl at school" unless she provided him with pictures. "Are you sure you want to drive to school tomorrow?" he asked, claiming that he saw her at school every day.[138]

The FBI initially contacted Dickerson believing that he might be one of Connolly's victims; they suspected that Connolly may have gained control over Dickerson's computer and used it to attack other computers as a way of hiding his tracks.[139] Soon, however, they realized that Dickerson himself was also behind the attacks, discovering evidence of hacking and videos of graphic, self-produced child pornography on his computer.[140] Dickerson also used a program that would allow him to search the Internet for vulnerable webcams that he might be able to hack.[141]

Dickerson explained to the FBI that he while he had never met Connolly in person, he had a good idea of his identity: as Dickerson's co-conspirator, Connolly referred to himself as "Lauren," and would often send Dickerson pictures of Connolly and information about Connolly's life.[142]

Dickerson was sentenced to 110 years in prison after pleading guilty to all charges: three counts of producing child pornography, one count of possessing child pornography, and two counts of computer fraud.[143] Connolly was charged with five counts of producing child pornography, six counts of extortion, and one count of computer fraud.[144] He pleaded guilty to one count of producing child pornography,[145] and was sentenced to 30 years in prison—though the sentencing judge declared, "If I could sentence you to life, I would."[146]

MICHAEL C. FORD

Investigators initially discovered Michael C. Ford when looking into an anonymous sextortionist whom they believed might be using a State Department IP address to obscure his identity.[147] As it happened, the IP address was not a ruse: the investigation ultimately traced the sextortion back to Ford, an employee at the U.S. Embassy in London.[148] Ford contacted his victims from his cubicle, storing elaborate spreadsheets of his victims' emails and passwords on his work computer.[149] His sextortion began the year he was hired at the Embassy; he was busy sextorting at work for six years without anyone at the Embassy noticing before he was finally arrested.[150]

Ford relied on a phishing scheme to gain his victims' passwords and steal explicit photos from their accounts, along with personal information such as the victims' addresses and phone numbers. He sent thousands of emails posing as a member of Google's "Account Deletion Team," notifying victims that their Google accounts were set to be deleted and requesting their passwords in order to prevent the purging of their account.[151] (Ford saved drafts of these phishing emails on his Embassy computer.)[152] He primarily targeted young women who belonged to college sororities or aspired to be models,[153] though in one case he sextorted a young man for a female friend's passwords.[154] The man refused to send along more pictures because, in his words, "I'm 16 in those photos [that Ford had already obtained] and if you post/distribute child porn, you're going to have a bad time." Ford responded, "Do you really think I care?"[155]

Once he obtained a victim's passwords and accessed her account, he would threaten to release her photos to family members or publish the photos on the Internet unless the victim provided him with video of women's changing rooms.[156] Sometimes, he would threaten to make public the victim's contact information and address as well.[157] In several cases he made good on his threats, at one point emailing a victim's mother a picture of her with a note reading, "Check out your little girl."[158] Some of his victims began to fear for their physical safety: one woman slept with a knife under her pillow, while another considered obtaining a gun to protect herself.[159]

Ford had successfully hacked into 450 computers and threatened 75 victims at the time of his arrest.[160] He was indicted on nine counts of cyberstalking, seven counts of computer fraud, and one count of wire fraud,[161] and pleaded guilty to all charges.[162] He was sentenced to 57 months in prison.[163]

CHRISTOPHER PATRICK GUNN AND JEREMY BRENDAN SEARS

Christopher Patrick Gunn had two methods of catfishing young girls to extort them for sexual photos.[164] In one, he would reach out through a fraudulent Facebook profile and pretend to be a new kid in town looking for friends—a ruse that conveniently explained away why his potential victim never would have heard of him before.[165] In his second method, he would contact girls over online chatting apps such as Omegle—a service that randomly pairs chatters for anonymous conversations[166]—and pretend to be none other than pop heartthrob Justin Bieber, roaming the Internet in the hopes of meeting his fans. As Bieber, he would offer free concert tickets or backstage passes to his young fans if they sent photos or video of their bare chests. He would then quickly move to make ever-more-invasive demands of his victims; if they initially sent a picture of their breasts, he would push for a full-body photo or a photo of the girls' friends bare-chested as well.[167]

Gunn was not alone in targeting young Beliebers as potential victims for sextortion. Jeremy Brendan Sears got his start in the "Bieber Hijacking and Trolling Company," an online group that trolled girls' fan-sites for Bieber and the boyband One Direction.[168] Soon, Sears struck out on his own, harassing the young website owners and spamming their pages in order to extort the girls for explicit photos and videos.[169] The fans, who had invested months or even years of work in collecting pictures of their idols, were desperate to regain control over their webpages—which was exactly what made them vulnerable to Sears.[170] Sears would also catfish victims using fake social media profiles and post victims' contact information online, promising to remove it only if the victims provided photographs or video.[171] When interviewed by the FBI, Sears stated that his sextortion had "a very minor sexual thing to it," but that the primary appeal was the "power" it offered him over his victims.[172]

Christopher Patrick Gunn was charged with six counts of producing child pornography, two counts of possessing child pornography, seven counts of stalking, 20 counts of extortion, and eight counts of interstate transmission in

aid of extortion.[173] He pleaded guilty to two counts of producing child pornography and four counts of extortion,[174] and was sentenced to 35 years in prison.[175]

Jeremy Brendan Sears received a sentence of 15 years[176] after pleading guilty to just one count of producing child pornography.[177] He was originally charged with 16 counts of producing child pornography, 11 counts of distributing or receiving child pornography, one count of possessing child pornography, one count of extortion, one count of computer fraud, and one count of aggravated identity theft.[178]

RICHARD FINKBINER

When FBI agents searched Richard Finkbiner's rural Indiana home in 2012, they discovered more than 22,000 video files saved on his computer, roughly half of which were sexually explicit and most of which depicted minors.[179] Finkbiner routinely sextorted so many people for these videos, he told the FBI, that it was impossible for him to recognize the images of any one particular victim that agents had presented to him: he had too many victims to recall them individually.[180]

Finkbiner would reach out to potential victims—usually teenage boys—through Omegle or other anonymous chatting programs. Like Chansler, he would ask them to strip and perform sexual acts while he surreptitiously recorded them, hiding his own identity by displaying sexually explicit videos in place of his own camera feed.[181] Then he would threaten to upload the video to pornographic websites unless the victims emailed him—and as soon as they did so, he would threaten to distribute the material to friends, family, and school acquaintances unless they agreed to become what he referred to as his "cam slaves."[182] In as many as three cases, Finkbiner may have used image editing software to trick his victims into believing that he had uploaded their videos to pornographic sites.[183]

At one point, a 17-year-old girl wrote to Finkbiner saying that she had attempted suicide the previous night and would attempt it again if he did not stop his requests. Finkbiner wrote back, "Glad i could help."[184]

When one boy protested against Finkbiner's requests, Finkbiner responded, "yes it is illegal im ok with that … i wont get caught im a hacker i covered my tracks."[185] In fact, he made no effort to hide his IP address, and the FBI was able to trace the email and Skype accounts he used for sextortion to the small Internet service company registered in his name.[186]

Overall, Finkbiner sextorted " "hundreds, if not thousands, of . . . minors and adults all over the world," prosecutors claimed.[187] Most of the victims were minors. He was charged with six counts of producing child pornography, 20 counts of interstate extortion, eight counts of interstate transmission in aid of extortion, two counts of possessing child pornography, and seven counts of stalking.[188] He pleaded guilty to all seven counts of stalking, two counts of producing child pornography, and 15 counts of extortion,[189] and was sentenced to 40 years in prison.[190]

ADAM SAVADER

Adam Savader, a college student active in Republican politics, spent the summer and fall of 2012 in a prestigious position as Paul Ryan's "sole intern" on the Romney-Ryan presidential campaign.[191] But by September 2012, he had begun sextorting,[192] targeting young women whom he knew from high school or college[193]—one of whom had threatened to take out a restraining order against him in the past.[194] In the case of one victim who was similarly

politically active, Savader threatened to release her photos to her mother, her sorority sisters, and the Republican National Committee.[195] He would usually goad his victims into responding to him: a typical series of messages reads, "I'm about to send those pics… Should I? If not tell me. I'm running out of patience… Answer me now or pay."[196]

Savader extorted at least 15 women in total,[197] hacking into victims' email and social media accounts in order to access sexually explicit photos stored there. His college and hometown connections with his victims allowed him access to their accounts, as he could reset their passwords by guessing the answers to security questions that asked about information such as high school mascots and street of residence.[198]

Once he had the photos, he would contact victims through Google Voice, a service that allows users to create a new number from which to receive and forward calls.[199] Savader's multiple Google Voice accounts allowed him to keep his cell phone number hidden from his victims, and may also have allowed him to prevent them from contacting him back in turn: Google Voice allows users to turn off call forwarding to their devices,[200] and one victim's account of her failed attempts to contact Savader is consistent with Savader's having used this function.[201] Savader used freshly created email accounts to register for the Google Voice numbers,[202] but both the forwarding number for the Google Voice accounts and the IP addresses used to create those email addresses traced directly back to Savader.[203]

Savader was sentenced to two-and-a-half years on one count of cyberstalking[204] after pleading guilty to one count of cyberstalking and one count of extortion;[205] he had originally been charged with four counts of each.[206] While in prison, Savader has registered a Super PAC lobbying for legislation supporting improved reintegration of previously incarcerated individuals into society. According to Savader's father, the PAC will refrain from fundraising until his son is released from prison.[207]

RINAT: ISRAELI CASE OF SEXTORTION

The problem of sextortion is not by any means limited to the United States. In 2013, a 30-year-old man was convicted in Israel of extortion, sexual harassment, and the publication of obscene material after posing as a female soldier on various social media sites and tricking young girls into communicating with him. Under pressure, the communications became sexually explicit and exploitative, with the offender requesting nude photos and other pornographic material from at least three minors.

In one instance, the perpetrator filmed a 13-year-old female minor without her knowledge over Skype after pressuring the girl to masturbate on camera. The young girl eventually attempted to end the relationship with the person she knew as "Rinat," cutting off communication with the offender. However, the man then told her that he had recorded all of their online conversations and would publish the material if she refused to continue their relationship. After the victim refused, the sextortionist published explicit images of the minor on Facebook.

> The court wrote: "The thought that children are unsafe in their own home is a difficult one, and it turns out that there, in their own room in their house under the watchful eye of their parents, the appellant managed to trick them, hurt them, and cause them unimaginable harm."

In another instance, the perpetrator pressed a different 13-year-old minor to engage in sexual acts over Skype. When the minor told the sextortionist that her mother was

in the room, he asked and eventually convinced his victim to pretend to change her clothes in front of her webcam, so as not to attract the attention of her mother, and to allow him to see her naked. According to the court opinion, the victim's mother was present in the room as she was sextorted.

In denying the man's appeal against the two-year prison sentence imposed on him, the Israeli Supreme Court stated, that "the appellant's action, absent any physical contact, does not reduce the severity of the offence." In a chilling conclusion, the court wrote: "The thought that children are unsafe in their own home is a difficult one, and it turns out that there, in their own room in their house under the watchful eye of their parents, the appellant managed to trick them, hurt them, and cause them unimaginable harm."[208]

IMPACT OF SEXTORTION ON VICTIMS

The harm that many victims experience as a result of sextortion is, indeed, unimaginable. But it is also real. Victims of sextortion feel a justified sense of powerlessness and vulnerability: they are at the mercy of their hackers. Victims have described descried feeling like a "slave" to the hackers during the sextortion scheme.[209] Victims of these schemes spend every moment in fear of the next message demanding more compromising pictures or videos, living in perpetual anxiety of the risk of public exposure. With every new picture sent to the hacker is the worry that it isn't enough or that the hacker will never leave. Related is the feeling of helplessness: the inability to reach out to others about what is going on for fear of the attacker's retaliation. The days, weeks, and months under the sextortionist's control can be an absolute "nightmare," where a victim is "trapped" and can't "talk to anyone."[210] One teenager told investigators that the experience "felt like I was being virtually raped."[211]

The traumatic effects on child victims can be particularly severe. Younger victims are sometimes paralyzed by the potential social repercussions of sextortion. One victim recounted that, as a young teenager, she was "already getting teased in middle school" and was terrified she might lose friends and become a target of cruel teenage bullying if her classmates found out what was going on.[212] The nature of sextortion also makes for easy victim-blaming: the victims, after all, took pictures and videos of themselves and sent them along. Why didn't they just refuse to go along with the scheme?

Martha Finnegan, an FBI expert in child forensics explains that this kind of psychological cruelty—forcing the victim to participate in the production of these images—can have "a devastating emotional effect" on the victims:

> [T]hat's what society doesn't get: Yes, the girls participated in this. But they're *children*; they're still very much victims. Even though they haven't been touched, the trauma level we see is as severe as hands-on offenses, because a lot of these kids don't know how to end what can go on, sometimes, for years. … And they think it's not happening to anyone else.[213]

Children are often the easiest targets of these sorts of crimes not only because of their social vulnerability, but because they often do not realize that what is happening is criminal behavior. They are often left defenseless and too scared to admit to their parents or to anyone else what is happening. They also sometimes have no idea when threats are completely idle ones. One young sextortion victim complied with demands for nude photos because her attacker threatened to "blow up" her computer if she did not, and the computer was a treasured new Christmas present.[214]

That defenselessness does not cease even in when the hacking is over and the sextortionist is prosecuted. One of Luis Mijangos' victims described the visceral fear of her hacker that has stayed with her since, despite Mijangos' prosecution and ultimate jail time: "He [still] haunts me every time I use the computer."[215] Another one of Mijangos' victims explained that moving away from the Los Angeles area has not made her feel any safer: as long as he had an Internet connection, Mijangos was able to attack from anywhere, at any time. This is a crime from which some victims have a great deal of trouble escaping. They carry the weight of this anxiety and distrust with them.

To make these points tangible, consider some of the victim impacts from the case studies in the previous section. In sentencing Abrahams, for example, the judge declared:

> Through his computer skills, he hacked into girls' computers and observed them in their bedrooms dressing and undressing through cameras, or webcams, on the computers. He hacked their e-mail and social media accounts, and by his own assessment attempted to make them his "slaves." The intimidation turned to extortion when he demanded that they perform certain acts before the computer camera or face posting of their images on the internet. He did in fact post images. And as one of the victims noted, she will never know for rest of her life when those images will resurface on the internet.[216]

In the Chansler case, impact statements for five victims and their family members were introduced at sentencing. One victim described herself as becoming a "hollow shell" under the onslaught of Chansler's demands, plagued by panic attacks.[217] The mother of another victim explained that her daughter now becomes uncomfortable whenever she steps out onto the street, constantly wondering if any passersby have seen her naked.[218] An FBI special agent assigned to the case described the situation of one young girl who was forced to leave school and move hundreds of miles away out of fear for her life, returning home only when she learned from FBI agents that Chansler had been arrested.[219]

Impact statements submitted in the Savader case make clear how an ever-present stream of threats can lead to victims' psychological exhaustion. One woman characterized the experience as an unending "barrage of harassment," leading to a "feeling of helplessness [that] consumed almost every aspect of my life."[220] Another described the extensive reach of Savader's sextortion:

> The harassment invaded every part of my life. There were times when I needed to completely turn my phone off to avoid receiving continuous harassment almost every minute. There was no way to block the messages because the numbers were constantly changing. I received messages on my cell phone while at home in Pennsylvania, in the classroom in D.C., and even on vacation with my family in Florida. The fake Facebook account then began contacting my mother, stepfather, brother, boyfriend, and best friend. The fake account sent messages to my family seeking further pictures of me. At this point, everyone in both my boyfriend's family and mine were involved. When the texts would not stop, I was forced to contact my cell phone provider and change my cell phone number.[221]

The sentencing transcript in the Ivory Dickerson case and the government's sentencing memorandum in the Finkbiner case makes for particularly ugly reading. In Dickerson's case, one victim reported that she became "afraid to go to school … afraid to walk outside" for fear that she would meet her tormenter.[222] The parents of a second victim testified that they constantly feared for their daughter's life: "we had no idea what would happen when she went to

the school, to the store, to anywhere."[223] The atmosphere of fear in the family was such that this second victim's younger brother began to worry that Dickerson would come and hurt him in his sleep.[224]

In Finkbiner, the government did not introduce victim impact statements. It did, however, lay out what Finkbiner made some of his victims do. In addition, as we noted above, to driving one girl to a suicide attempt, he forced children to engage in all sorts of highly-degrading sexual activity. The following is an almost random sample:

C. Finkbiner's Victimization of John Doe 2 (Count 2 of the First Information)

At the time of Finkbiner's offense against him, John Doe 2 was a 14-year-old boy located in Sissonville, West Virginia. During a March 10, 2011, video chat session, Finkbiner demanded that John Doe 2 model a jock strap, dance naked, do sit-ups, masturbate and eat his ejaculate, and penetrate his anus with a finger. John Doe 2 complied with Finkbiner's demands, which Finkbiner recorded on video.

During a March 14, 2011, video chat session, Finkbiner demanded that John Doe 2 wear short shorts, strip naked, dance, masturbate, wear a wet t-shirt and jock strap, dance, strip again, do sit-ups and simulate sex with a pillow. John Doe 2 again complied with Finkbiner's demands, which Finkbiner recorded on video.

During a March 16, 2011, video chat session, Finkbiner demanded that John Doe 2 do a strip dance, masturbate, wear his jock strap backwards, dance, get naked again, do push-ups and masturbate again. John Doe 2 again complied with Finkbiner's demands, which Finkbiner recorded on video.

D. Finkbiner's Victimization of John Doe 3 (Count 3 of the First Information)

At the time of Finkbiner's offense against him, John Doe 3 was a 14-year-old boy located in Dubuque, Iowa. During a May 10, 2011, chat session, Finkbiner recorded a video of John Doe 3 masturbating.

During another video chat session about an hour later, John Doe 3 initially refused to show Finkbiner his face on camera. Finkbiner stated that he knew John Doe 3 lived in Dubuque, Iowa, and threatened to send the video to named individuals and teachers who knew John Doe 3, and a named high school. John Doe 3 then agreed to comply with Finkbiner's demands. During this chat session, Finkbiner demanded that John Doe 3 strip, dance, masturbate, and show Finkbiner his anus. John Doe 3 complied with Finkbiner's demands, which Finkbiner recorded on video.

E. Finkbiner's Victimization of John Doe 4 (Count 4 of the First Information)

At the time of Finkbiner's offense against him, John Doe 4 was a 15-year-old boy located in River Falls, Wisconsin. During a May 12, 2011, video chat session, Finkbiner recorded a video of John Doe 4 masturbating.

During another video chat session about 20 minutes later, Finkbiner demanded that John Doe 4 be his "cam slave" and engage in additional sexually explicit conduct on video. John Doe 4 initially refused to comply. Finkbiner threatened to send the video to individuals and teachers who knew John Doe 4, naming the individuals and a high school. John Doe 4 then agreed to comply with Finkbiner's demands. Finkbiner demanded that John Doe 4 dance like "a stripper," masturbate, and show Finkbiner his anus. Finkbiner demanded that

John Doe 4 play with his nipples, then lay in bed and masturbate. Finkbiner then told John Doe 4 to ejaculate into his hand, lick up his ejaculate and show his mouth full of ejaculate to Finkbiner on camera. John Doe 4 complied with Finkbiner's demands, which Finkbiner recorded on video.

Finkbiner then told John Doe 4 to contact him again the next day. John Doe 4 pleaded with Finkbiner not to have to engage in any more activity on camera. Finkbiner stated "complain and ill fukk u over," "depends on u." John Doe 4 then asked Finkbiner to just get it all done at that time, Finkbiner stated "ull be fine dgo do ur hw or somthing." John Doe 4 continued to plead with Finkbiner, stating "no please im scared i dont wanna worry about this please." Finkbiner did not respond further to John Doe 4.[225]

CONCLUSION

The discussion above suggests a number of important policy and social interventions. Our purpose in this paper is largely to describe a serious problem of whose existence many people are unaware. But to describe this problem is also to notice serious deficiencies in the way we are addressing the matter as a society. The following are several recommendations aimed at different levels of society:

RECOMMENDATIONS FOR LAWMAKERS

The law currently contains two startling deficiencies that lead to serious sentencing disparities in sextortion cases. The first is the absence of any parallel in cases involving adult victims for the severe sentencing associated with federal child pornography prosecutions. The disparity is understandable as an original matter: adult pornography is, as a general matter, constitutionally protected speech and expression, whereas the federal government has an abiding interest in protecting children against exploitation in fashions that implicate federal jurisdiction. In this context, however, as we have explained, the disparate treatment of adults and children results in a gross under-protection of adult women relative to children of either gender in the interstate coerced production of pornography. Exacerbating this problem is the relative weakness of many state laws. Some serious sextortion cases we reviewed were prosecuted at the state level as misdemeanors.

> Prosecutors and investigators should operate on the presumption that sextortion is taking place everywhere and should devote human resources to investigating and prosecuting sextortion cases as part of their broader focus on child exploitation.

Recommendation #1: Given that these cases are numerous, many are interstate in nature, and most being prosecuted federally anyway, Congress should consider adopting a federal sextortion statute that addresses the specific conduct at issue in sextortion cases and does not treat the age of the victim as a core element of the offense. Specifically, as we lay out in greater depth in a separate paper, "Closing the Sextortion Sentencing Gap," we believe this statute should combine elements of the federal interstate extortion statute with elements of the aggravated sexual abuse statute and have sentencing that parallels physical-world sexual assaults.

Recommendation #2: State lawmakers should likewise adopt strong statutes with criminal penalties commensurate with the harm sextortion cases do. More broadly, states should carefully review their statutes relative to the production

and distribution of non-consensual pornography. Many states have no such laws. Others have laws of inadequate force. In our view, states should both criminalize the production and distribution of nonconsensual pornography and give victims of it reasonable civil remedies against their victimizers. In combination with a federal statute, this would create a number of avenues for victims to pursue.

RECOMMENDATIONS FOR FEDERAL AUTHORITIES

Short of the adoption of new legislation, there are important steps available to the Justice Department and the FBI to take administratively. One striking feature of the sextortion problem is that nobody knows how widespread or serious it is, because nobody publishes good data on sextortion cases at either the state or federal levels. The failure to lack of readily available data takes place even as the FBI has repeatedly warned of the problem and even as the Justice Department has announced Project Safe Childhood, which the department describes as "a Department of Justice initiative launched in 2006 to combat the proliferation of technology-facilitated crimes involving the sexual exploitation of children."[226] A number of Justice Department press releases in sextortion cases describe the prosecutions in question as taking place under the Project Safe Childhood umbrella. It is striking that even the project under which sextortion prosecutions take place cannot readily identify or count them.

Moreover, the federal system is notably uneven in its focus on sextortion cases. We think it unlikely that four of our cases come each from such jurisdictions as the Central District of California, the Middle District of Florida, and the Northern District of Georgia because these jurisdictions are particularly rife with sextortionists. We suspect, moreover, that the reason three of our cases come from state court in Wisconsin has more to do with the attention in that state of a single local prosecutor named Erin Karshen—who cares about the issue—than with the prevalence of the offense in Milwaukee. We also suspect that the apparent absence of cases (at least in our dataset) from such powerhouse prosecutorial districts as the Southern and Eastern Districts of New York does not reflect the fact that New York City is a sextortion-free zone.

Recommendation #3: The federal government should develop and maintain robust data on federal prosecutions of sextortion and other cases involving the non-consensual production of pornography and cyberstalking. It should not wait to do so until Congress passes statutes specifically criminalizing sextortion. The conduct is all already covered by federal statutes; it is mostly prosecuted, as we have seen, in federal court. Having access to good data on federal handling of these cases is critical both to raising awareness of the problem and to developing more refined statutory tools for addressing it.

Recommendation #4: U.S. Attorneys and FBI Special Agents in Charge in jurisdictions which have not seen these cases should not conclude that they are not taking place but that they have probably overlooked them. Prosecutors and investigators should operate on the presumption that sextortion is taking place everywhere and should devote human resources to investigating and prosecuting sextortion cases as part of their broader focus on child exploitation.

Recommendation #5: They should also adopt as policy what is already de facto practice: Federal authorities, being both better positioned for interstate and international investigations than state or local authorities and having the stronger laws and penalties, should presume—in contrast to many other sex crimes cases—that they are an investigative and prosecutorial front line. Unlike physical sexual assaults, which are presumptively local in nature, sextortions take place in a domain that is generally non-local and often requires complex interjurisdictional machinations and technical forensics. These cases are, much of the time, best handled at the federal level.

RECOMMENDATIONS FOR DEVICE MANUFACTURERS AND INTERNET COMPANIES

Webcams are a great innovation for human connectivity. They are also often insecure and offer sextortionists and other bad cyber actors literal visibility into the activity of non-consenting targets. Similarly, relatively lax password controls—and relatively simple password recovery—on social media platforms makes hacking accounts too easy.

Recommendation #6: Hardware manufacturers should build into computers easy slip-over webcam masks that allow users to physically cover their computers' camera when it is not in use. More generally, hardware manufacturers should consider whether the security risks of software-driven webcams exceed the convenience benefits and whether a physical switch disabling webcams should be the preferred norm. By one means or another, computer manufacturers should make it convenient and easy to physically disable when not in use those hardware devices that hackers can use to turn computers into surveillance devices.

Recommendation #7: Account hacking would be far more difficult if Internet and social media companies required the use of strong passwords and made those passwords recoverable based on criteria other than data hometown stalkers know well or can guess easily.

RECOMMENDATIONS FOR PARENTS AND TEACHERS AND VICTIMS

One of the factors that makes sextortion cases, particularly those involving child victims, difficult to uncover is the intergenerational gap in sexual mores concerning online activities. Teenagers often send nude pictures of themselves to one another. Their parents find this shocking. And this gap in attitude inhibits communication between generations when what a teenager may regard as innocent sexting suddenly turns very ugly.

Yet one of the features of these cases that jumps out at even a casual reader is how much better those victims who have an adult to turn to fare than those who are too humiliated to tell a parent or a teacher what is happening to them. Parents are better positioned to activate law enforcement than are children. And every sextortionist who gets caught has one thing in common: a victim who talked to someone that victim decided to trust. This observation has important process implications.

Recommendation #8: It is critically important for parents and teachers to establish with their children a no-judgment, no-questions reporting regime for sexual exploitation online. Children need to understand that there are ways out of the traps the sextortionists have them in. And responsible adults need to create mechanisms the children they are responsible for feel safe using when they are threatened.

Finally, there is one critical recommendation with respect to victims of sextortion, both those currently subject to it and those who have been victimized in this past.

Recommendation #9: Victims need to be enabled to come forward and, to the extent they wish, speak up. Current victims of sextortion may or may not understand that the person victimizing them may also be doing the same thing to literally hundreds of other people and will not stop until someone gets law enforcement involved. Past victims have a role to play in making current victims understand that they are experiencing something that is both common and not their fault. Yet it can be extremely difficult for victims to come forward, especially in the absence of assurances

that the law will protect them and that law enforcement will treat them with respect and dignity. In this context, it is especially troubling that child pornography laws in many jurisdictions have been used to punish minors for creating images of themselves—a reality that means that minor victims potentially put themselves in legal jeopardy by coming forward. Only by making it possible to talk about sextortion will society lessen the power of those who engage in it.

ENDNOTES

1 * We are grateful for extremely helpful comments and assistance from Chris Jay Hoofnagle, Hannah Neprash, Jonathan Rauch, Mary Anne Franks, Carrie Goldberg, Danielle Citron, Erin Karshen, Wells Bennett, and Staley Smith.

2 Government's Objections to the PSR and Sentencing Position at 21, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 20, 2011).

3 Complaint at 13, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. June 17, 2010).

4 *Id.* at 12.

5 *Id.*

6 Affidavit for Search Warrant at 9, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. Mar,. 2010).

7 Indictment at 2, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 8, 2010).

8 Government's Objections to the PSR and Sentencing Position at 3, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 20, 2011).

9 Indictment at 3, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 8, 2010).

10 *Id.*

11 *Id.* at 5.

12 Government's Objections to the PSR and Sentencing Position at 5, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 20, 2011).

13 Indictment at 4, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 8, 2010).

14 *See Id.* at 6. *See also* Complaint at 9, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. June 17, 2010); Government's Objections to the PSR and Sentencing Position at 4, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 20, 2011).

15 *See* Indictment at 4, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 8, 2010); Government's Objections to the PSR and Sentencing Position at 1, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 20, 2011).

16 *Id.*

17 *Id.* at 1, 18.

18 Complaint at 16, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. June 17, 2010).

19 David Kushner, *The Hacker is Watching*, GQ Magazine (Jan. 11, 2012), http://www.gq.com/story/luis-mijangos-hacker-webcam-virus-internet.

20 Complaint at 10, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. June 17, 2010).

21 *Id.*

22 Government's Objections to the PSR and Sentencing Position at 21, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 20, 2011).

23 Indictment at 4, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 8, 2010).

24 Complaint at 8, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. June 17, 2010).

25 Government's Objections to the PSR and Sentencing Position at 1, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. July 20, 2011).

26 *Id.*

27 *Id.* at 16.

28 *Id.*

29 *Id.* at 17.

30 "Orange County Man Suspected of Hacking Computers Arrested on Federal Charges Related to Demands for Sexually Explicit Videos from Women and Teenage Girls," U.S. Attorney's Office, Central District of California, June 22, 2010. Accessed on March 8, 2016 (https://www.fbi.gov/losangeles/press-releases/2010/la062210a.htm)

31 *See* Plea Agreement, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. Mar. 11, 2011).

32 *See* Judgment, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. Sept. 16, 2011).

33 Complaint at 7, United States v. Mijangos, No. 10-743-GHK (C.D. Cal. June 17, 2010).

34 Marisol Bellow, *'Sextortion' is an Online 'Epidemic' Against Children*, USA Today (July 2, 2014), http://www.usatoday.com/story/news/nation/2014/07/01/sextortion-teens-online/11580633/.

35 Conversation with Elishe Julian Wittes.

36 State of Rhode Island v. Joseph Simone, No. P2-2012-0684A (Providence County Superior Court). *See also* W. Zachary Malinowski, *Former Moses Brown Wrestling Coach Sentenced for Child Pornography, Indecent Solicitation of Minor and Extortion*, Providence Journal (Dec. 12, 2014), http://www.providencejournal.com/article/20141212/news/312129915.

37 United States v. Adam Savader, No. 13-20522-MOB-PJK (E.D. Mich.).

38 *See, e.g.*, United States v. Killen, No. 15-20106-KMM-1 (S.D. Fla.); United States v. Finkbiner, No. 12-00021-WTL-CMM-1 (S.D. Ind.). *See also* Matt Hennie, *Teen Tried Suicide During Sextortion by Ga. Man*, Project Q Atlanta (May 5, 2015), http://www.projectq.us/atlanta/teen_tried_suicide_during_sextortion_by_ga._man?gid=13497.

39 *See* United States v. Ralph Daniel Smith, No. 15-00342-BKS-1 (N.D.N.Y.); United States v. Russell Freed, No. 11-00132-TFM (W.D. Pa.). See comment on note 36.

40 Benjamin Wittes, Cody Poplin, Quinta Jurecic & Clara Spera, *Closing the Sextortion Sentencing Gap: A Legislative Proposal*, Brookings (May 11, 2016), http://www.brookings.edu/research/reports2/2016/05/sextortion-sentencing-wittes-poplin-jurecic-spera

41 *See, e.g.*, Charles Wilson, *Online 'Sextortion' Of Teens On The Rise: Feds*, Associated Press (Oct. 14, 2010), http://www.huffingtonpost.com/2010/08/14/online-sextortion-of-teen_n_682246.html; Kristine Johnson, *Analyzing The Disturbing World of 'Sextortion',* CBS New York (Nov. 1, 2010), http://newyork.cbslocal.com/2010/11/01/analyzing-the-disturbing-world-of-sextortion/.

42 *'Sextortion' Charges To Come Up Next Week*, Los Angeles Times (Apr. 5, 1950), archived at http://pqasb.pqarchiver.com/latimes/doc/166101610.html?FMT=CITE&FMTS=CITE:AI&type=historic&date=Apr%2005,%201950&author=&pub=Los%20Angeles%20Times&edition=&startpage=&desc=%27SEXTORTION%27%20CHARGES%20TO%20COME%20UP%20NEXT%20WEEK.

43 *See, e.g.*, Press Release, U.S. Attorney's Office for the Eastern District of Virginia, Virginia Man Sentenced to 24 Years for Sextortion of Minors on Facebook (Sept. 25, 2014), https://www.fbi.gov/richmond/press-releases/2014/virginia-man-sentenced-to-24-years-for-sextortion-of-minors-on-facebook.

44 Kate Murphy*, In Online Dating, 'Sextortion' and Scams*, New York Times (Jan. 15, 2016), http://www.nytimes.com/2016/01/17/sunday-review/in-online-dating-sextortion-and-scams.html?_r=1.

45 Sheryl Gay Stolberg and Richard Pérez-Peña, *Wildly Popular App Kik Offers Teenagers, and Predators, Anonymity,* New York Times (Feb. 5 2015), http://www.nytimes.com/2016/02/06/us/social-media-apps-anonymous-kik-crime.html.

46 Michael Joseph Gross, *Sextortion at Eisenhower High*, GQ Magazine (Jun. 30, 2009), http://www.gq.com/story/wisconsin-high-school-sex-scandal-online-facebook.

47 David Kushner, *The Hacker is Watching*, GQ Magazine (Jan. 11, 2012), http://www.gq.com/story/luis-mijangos-hacker-webcam-virus-internet.

48 Bill Rankin, *Predators Exploit Social Sites for 'Sextortion' of Minors*, Atlanta Journal-Constitution (May 4, 2013), http://www.myajc.com/news/news/local/predators-exploit-social-sites-for-sextortion-of-m/nXhBK/?icmp=ajc_internallink_invitationbox_apr2013_ajcstubtomyajcpremium; Dan Sewell, *Ohio Cases Highlight Online Targeting, 'Sextortion' of Teens*, Associated Press (Oct. 25, 2015), http://bigstory.ap.org/article/910f6bff282e491295b75

efcdd4936b4/ohio-cases-highlight-online-targeting-sextortion-teens; Marisol Bello, *'Sextortion' is an Online 'Epidemic' Against Children*, USA Today (July 2, 2014), http://www.usatoday.com/story/news/nation/2014/07/01/sextortion-teens-online/11580633/.

49 *See* Digital Citizens Alliance , Selling "Slaving": Outing the Principal Enablers that Profit from Pushing Malware and Put Your Privacy at Risk (July 2015), https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/07027202-8151-4903-9c40-b6a8503743aa.pdf.

50 Darcy Katzin et al., *Social Networking Sites: Breeding Grounds for "Sextortion" Prosecutions*, U.S. Att'y's Bull., Sept. 2011, at 54–58, http://www.justice.gov/usao/eousa/foia_reading_room/usab5905.pdf.

51 *Cyber Alert for Parents & Kids, Tip #2: Beware of 'Sextortion'* (Feb. 2, 2010), https://www.fbi.gov/news/stories/2012/february/sextortion_021012; *see also Special Agent Nickolas Savage Dicusses 'Sextortion'* (last accessed Mar. 24, 2016), https://www.fbi.gov/news/stories/2012/february/sextortion_021012/special-agent_021012.

52 *Oversight Hearing of the Federal Bureau of Investigation: Before the H. Comm. on the Judiciary*, 113th Cong. 19 (2013) (statement of Robert S. Mueller, III, Director, Federal Bureau of Investigation).

53 *Sextortion: Help Us Locate Additional Victims of an Online Predator* (July 7, 2015), https://www.fbi.gov/news/stories/2015/july/sextortion.

54 *What is Sextortion?* (July 7, 2015), https://www.fbi.gov/news/stories/2015/july/sextortion/video/what-is-sextortion.

55 *FBI This Week: Sextortion Reports on the Rise* (July 7, 2015), https://www.fbi.gov/news/podcasts/thisweek/sextortion-reports-on-the-rise.mp3/view.

56 Federal Bureau of Investigation, STOP SEXTORTION: Sextortion of Children in the United States, A Fact Sheet for Parents and Children, (July 2015), https://www.fbi.gov/news/stories/2015/july/sextortion/stop-sextortion-brochure.

57 *See* Tracy Webb, *The Brave New World of Cyber Crime Investigation and Prosecution*, 19 Nexus J. Op. 77, 82–83 (2013/2014) (discussing sextortion—defined as "extortion using sexual images"—briefly in the context of a wider paper about the development of cybercrime in the new social media age); Clay Calvert et al., *Playing Legislative Catch-Up in 2010 With a Growing, High-Tech Phenomenon: Evolving Statutory Approaches for Addressing Teen Sexting*, 11 PGH. J. Tech. L. & Pol'y 1, 56–57 (2010) (noting in the conclusion that sextortion is a growing phenomenon to which lawmakers should pay attention); Sherry Capps Cannon*, OMG! "Sexting": First Amendment Right or Felony?*, 38 S.U. L. Rev. 293, 295 (2011) (mentioning sextortion as an "alarming trend" in the broader context of sexting and the advent of technology); Laure E. Gomez-Martin, *Smartphone Usage and the Need for Consumer Privacy Laws*, 12 PGH. J. Tech. L. & Pol'y 2, P12 (2012) (referencing sextortion very briefly and in general terms).

58 Susan Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes 87*,* (Northeastern University Pres,s 2012).

59 *See* Danielle Keats Citron, Hate Crimes in Cyberspace, (Harvard University Press, 2014). Citron's book focuses on cases involving the denial of economic, social, and political opportunities we tend to associate with civil rights.

Moreover, sextortion often involves minors, whereas Citron's book focuses on the ways in which cyber harassment and stalking deprives adult women, particularly young women, of important life opportunities.

60 Email from Tracey Kyckelhahn, PhD, Statistician at Bureau of Justice Statistics (Sept. 15, 2015).

61 Email from Federal Bureau of Investigation Office of Public Affairs (Sept. 9, 2015)) (linking to webpage on VCAC program, https://www.fbi.gov/about-us/investigate/vc_majorthefts/cac/overview-and-history (last accessed Mar. 29, 2016)).

62 Email from Peter Carr, Spokesman for the Dep't of Justice (Sept. 11, 2015).

63 Email from Mary Anne Franks, Associate Professor of Law at the University of Miami School of Law and Vice President of the Cyber Civil Rights Initiative (Sept. 2015); Email from Carrie Goldberg, Founding Attorney at C. A. Goldberg, PLLC and Board Member and Volunteer Attorney at the Cyber Civil Rights Initiative (Sept. 2015).

64 Email to Elisa D'Amico, Partner at K&L Gates and Co-Founder of the Cyber Civil Rights Legal Project (Sept. 2015).

65 Email to Family Online Safety Institute (Sept. 2015).

66 Email from Thorn: Tech Innovation to Fight Child Sexual Exploitation (Sept. 2015).

67 Email to National Center for Missing and Exploited Children (Sept. 2015).

68 National Center for Missing and Exploited Children, *Sextortion* (last accessed Apr. 12, 2015), http://www.missingkids.org/Sextortion/.

69 *See, e.g.* United States v. Tyler Schrier, Keith James Hudson, and Ryder Finney, No. 11-01175-SJO (C.D. Calif.); People v. Kevin Bollaert, No. CD252338 (Sup. Ct. of Calif., San Diego County).

70 Manuel Mogato, *Philippines Dismantles International 'Sextortion' Gangs with Massive Arrest Sweep,* Reuters (May 2, 2014), http://www.huffingtonpost.com/2014/05/02/philippines-sextortion-raids_n_5251413.html.

71 The cases included in this study are: United States v. Jonathan Vance, No. 08-00194-WHA-CSC(M.D. Ala.); United States v. Jared James Abrahams, No. 8:13-CR-00199 (C.D. Ca.); United States v. Luis Mijangoes, No. 2:10-CR-00743 (C.D. Ca.); United States v. Karen Kazaryan, No. 2:13-CR-56 (C.D. Ca.); United States v. Jeremy Brendan Sears, No. 2:14-CR-00274 (C.D. Ca.); United States v. Jason Betensky, No. 3:11-CR-00015 (D. Conn.); United States v. Joshua Blankenship, No. 8:11-CR-00461 (D. Md.); United States v. Marc Joseph Punzalan, No. 8:14-CR-00252 (D. Md.); United States v. James F. Connor V, No. 1:15-CR-10398 (D. Mass.); United States v. Anton Martynenko, No. 0:16-CR-00013 (D. Minn.); United States v. Theodore J. Castine, No. 6:11-CR-00020 (D. Mont.); United States v. Ryan J. Vallee, No. 1:15-CR-115-01-PB (D. N.Hamp.); United States v. John Bryan Villegas, No. 1:13-CR-00075-JL (D. N. Hamp.); United States v. Bryan Jacobs, No. 1:10-CR-801 (D.N.J.); United States v. Dustin Coleman, No. 3:14-CR-4 (D. N. Dak.); United States v. Mario Lebron-Caceres, No. 3:15-CR-00279 (D.P.R.); United States v. Jimmy Caraballo-Colon, No. 3:13-CR-00383 (D.P.R.); United States v. Mark Robert Reynolds, No. 4:14-CR- 00547 (D.S.C.), United States v. Garrett Drew Roegner, No. 4:14-CR-00547 (D.S.C.); United States v. Brian Caputo, No.

14-CR-00041 (E.D. Ca.); United States v. Jordan James Kirby, No. 14-CR-225 (E.D. Ca.); United States v. Sungkook Kim, No. 6:08-CR-00134 (E.D. Kent.); United States v. John Michael Fowler, No. 2:14-CR-290 (E.D. La.); United States v. Adam Paul Savader, No. 2:13-CR-20522-MOB-PJK (E.D. Mich.); United States v. Nicholas Glenn Wilcox, No. 2:15-CR-20682 (E.D. Mich.); United States v. Christopher Steibing, No. 2:14-CR-00256-HB (E.D. Penn.); United States v. Nicholas Joseph Rotundo, No. 4:14-CR-166 (E.D. Tex.); United States v. Cameron Scot Bivins-Breeden, No. 3:14-CR-00057 (E.D. Va.); United States v. Daniel Chase Harris, No. 2:14-CR-00076-MSD-DEM (E.D. Va.); United States v. Christopher Patrick Gunn, No. 2:12-CR-064 (M.D. Ala.); United States v. Melvin Barber Bridgers III, No. 8:14-CR-00445 (M.D. Fla.); United States v. Lucas Michael Chansler, No. 3:10-CR-00100 (M.D. Fla.); United States v. Patrick Connolly, No. 6:09-CR-00047 (M.D. Fla.); United States v. Ivory Dickerson, No. 6:06-CR-00238, 6:07-CR-150-ORL-22UAM (M.D. Fla.); United States v. Matthew C. Walker, No. 3:15-CR-00119-BAJ-EWD (M.D. La.); United States v. Corey Gallisdorfer, No. 1:12-CR-00001-WO-1 (M.D. N. Caro.); United States v. Joseph J. Ostrowski, No. 3:12-CR-00131-EMK (M.D. Penn); United States v. Tremain Hutchinson, No. 1:12-CR-00409 (N.D. Georgia); United States v. Michael Ford, No. 1:15-CR-00319 (N.D. Georgia); United States v. Michael Macaluso, No. 1:09-CR-170 (N.D. Georgia), United States v. Destin Whitmore, No. 1:14-cr-00054-CAP-GGB (N.D. Georgia); United States v. Brian Newman, No. 3:12-CR-69 (N.D. Ind.); United States v. Ralph Daniel Smith, No. 15-CR-342 (N.D.N.Y.); United States v. William T. Koch, No. 1:13-CR-70 (N.D. Ohio); United States v. Gregory Bogomol, No. 4:14-CR-00174 (N.D. Tex.); United States v. Joshua James Geer, No. 4:13-cr-00036-HLM-WEJ-1 (N.D. Georgia); United States v. Jesus Javier Hernandez Carvajal, No. 1:15-CR-20595 (S.D. Fla.); United States v. Patrick Killen, No. 15-CR-20106 (S.D. Fla.); United States v. Richard Leon Finkbiner, No. 2:12-CR-00021 (S.D. Ind.); United States v. Trevor Shea, No. 1:10-CR-00096-WTL-DKL (S.D. Ind.); United States v. Austin Williams, No. 1:13-CR-226 (S.D. Ind.); United States v. Bryan Harris, No. 1:15-CR-108 (S.D. Ohio); United States v. Cody Lee Jackson, No. 1:15-CR-118-MRB-1 (S.D. Ohio); United States v. Nicholas Kurtz, No. 1:15-CR-107 (S.D. Ohio); United States v. Jorge Juan Perez, No. 4:10-CR-00855 (S.D. Tex.); United States v. Jesse S. Williams, No. 1:14-CR-5 (W.D. Kent.); United States v. James Allen, No. 1:13-CR-00022 (W.D.N.Y.); United States v. Russell Freed, No. 2:11-CR-00132-TFM (W.D. Penn.); United States v. Michael Martinez, No. 15-CR-973 (W.D. Tex.); United States v. Kai Lundstroem Pedersen, No. 4:10-CR-257 (W.D. Miss.); United States v. Wesley Brandt, No. 8:11-CR-58 (M.D. Fla.); United States v. Lucas Robinson, No. 1:12-CR-89 (N.D. Iowa); United States v. Christopher DeKruif, No. 4:15-CR-20143-LJM-MJH (E.D. Mich.); Colorado v. Gregory Kasarcik (Jefferson County), see (http://jeffco.us/district-attorney/news/2015/gregory-kasarcik-sentenced-for-sexual-exploitation-of-a-child/); California v. Cesar Mauricio Estrada-Davila, No. MA066758 (Los Angeles); Wisconsin v. Gerardo Diaz Chavez, No. 2015CF004500 (Milwaukee); Wisconsin v. Cameron Wiley, No. 2015CM369 (Milwaukee); Wisconsin v. Justin Tunks, No. 2015CF003012 (Milwaukee); Florida v. Jarrod James Williams, No. 2015 CF 001627 (Osceola County); Missouri v. Denis Aguilar, No. 14AE-CR01664-01 (Platte County); Florida v. Daniel Dunfee, No. 2015CF003934A000XX (Polk County); Rhode Island v. Joseph Simone, No. P2-2012-0684A (Providence); New Jersey v. Miguel Angel Moran (Somerset County), see (http://www.nj.com/somerset/index.ssf/2015/02/bound_brook_man_indicted.html); Kentucky v. Chase Coston (Warren County), see (http://www.bgdailynews.com/news/man-charged-in-internet-slaving-case-accused-of-coercing-juvenile/article_294abd2d-510c-5975-9f21-e8f27d523132.html); Wisconsin v. Anthony Stancl, No. 68041000028558 (Waukesha County); Plony (John Doe) v. The State of Israel, Crim. App. 2656/13; Eduardo Arturo Romero Barrios (Mexico), see (https://www.ice.gov/news/releases/255-child-predators-arrested-61-victims-identified-during-operation-iguardian); and Aydin Coban (Netherlands), see (http://www.cbc.ca/news/canada/british-columbia/amanda-todd-aydin-coban-not-charged-1.3290147).

72 The jurisdictions in which sextortion cases were prosecuted are: Alabama Middle District, Central District of California, District of Connecticut, District of Maryland, District of Massachusetts, District of Minnesota, District of Montana, District of New Hampshire, District of New Jersey, District of North Dakota, District of Puerto Rico, District

of South Carolina, Eastern District of California, Eastern District of Kentucky, Eastern District of Louisiana, Eastern District of Michigan, Eastern District of Pennsylvania, Eastern District of Texas, Eastern District of Virginia, Middle District Alabama, Middle District of Florida, Middle District of Louisiana, Middle District of North Carolina, Middle District of Pennsylvania, Northern District of Georgia, Northern District of Indiana , Northern District of New York, Northern District of Ohio, Northern District of Texas, Southern District of Florida, Southern District of Indiana, Southern District of Ohio, Southern District of Texas, Western District of Kentucky, Western District of New York, Western District of Pennsylvania, Western District of Texas, Western District of Missouri, Northern District of Iowa, Jefferson County (Colorado), Los Angeles County (California), Milwaukee County (Wisconsin), Osceola County (Florida), Platte County Circuit Court (Missouri), Polk County (Florida), Providence Superior Court (Rhode Island), Somerset County (New Jersey), Warren County (Kentucky), Waukesha County (Wisconsin), Israel, Netherlands, and Mexico.

73 The states and territories in which these cases were prosecuted include: Alabama, California, Colorado, Connecticut, Florida, Georgia, Indiana, Iowa, Kentucky, Louisiana, Massachusetts, Maryland, Minnesota, Mississippi, Missouri, Montana, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, Texas, Virginia, and Wisconsin.

74 The cases involving only minor victims involve defendants Jeremy Brendan Sears, Jason Betensky, Joshua Blankenship, Marc Joseph Punzalan, Anton Martynenko, Theodore J. Castine, Ryan J. Vallee, Bryan Jacobs, Dustin Coleman, Jimmy Caraballo-Colon, Mark Robert Reynolds, Brian Caputo, Jordan James Kirby, John Michael Fowler, Nicholas Glenn Wilcox, Christopher Steibing, Cameron Scot Bivins-Breeden, Daniel Chase Harris, Plony (John Doe), Gregory Kasarcik, Cesar Mauricio Estrada-Davila, Eduardo Arturo Romero Barrios, Christopher Patrick Gunn, Lucas Michael Chansler, Patrick Connolly, Matthew C. Walker, Corey Gallisdorfer, Gerardo Diaz-Chavez, Cameron Wiley, Tremain Hutchinson, Michael Macaluso, Destin Whitmore, Brian Newman, Ralph Daniel Smith, William T. Koch, Gregory Bogomol, Joshua James Geer, Jarrod James Williams, Denis Aguilar, Daniel Dunfee, Joseph Simone, Miguel Angel Moran, Jesus Javier Hernandez Carvajal, Patrick Killen, Trevor Shea, Austin Williams, Bryan Harris, Cody Lee Jackson, Nicholas Kurtz, Jorge Juan Perez, Chase Coston, Jesse S. Williams, Kai Lundstroem Pedersen, Wesley Brandt, and Lucas Robinson.

75 The cases included in this study involving both minor victims and adult victims include: Jonathan Wryn Vance, Jared James Abrahams, Luis Mijangos, Sungkook Kim, Melvin Barber Bridgers III, Ivory Dickerson, Joseph J. Ostrowski, Aydin Coban, Richard Leon Finkbiner, Anthony Stancl, James Allen, Russell Freed, Michael Martinez, and Christopher DeKruif.

76 The cases included that involve all adult victims are: Karen Kazaryan, James F. Connor V, John Bryan Villegas, Mario Lebron-Caceres, Adam Paul Savader, Nicholas Joseph Rotundo, Justin Tunks, Michael Ford, Garrett Drew Roegner.

77 There is only one case in our study sample in which all victims are adults and the victim population is mixed gender, that of Michael Ford. There are at least five other cases in which there are both adult victims and male victims, though it is not clear how many of the victims are both adult and male in those cases. Those cases involve defendants Joseph J. Ostrowski, Anthony Stancl, Richard Leon Finkbiner, Christopher DeKruif, and Aydin Coban.

78 The cases that involve minor victims in which all identified victims are male include those of: Jason Betensky, Anton Martynenko, Bryan Jacobs, Nicholas Glenn Wilcox, Corey Gallisdorfer, Gerardo Diaz-Chavez, Michael Macaluso, William T. Koch, Gregory Bogomol, Joseph Simone, Patrick Killen, Joseph J. Ostrowski, and Anthony Stancl.

79 The cases in this study that involve minors and both males and females include those of: Jeremy Brendan Sears, John Michael Fowler, Eduardo Arturo Romero Barrios, Tremain Hutchinson, Joshua James Geer, Aydin Coban, Richard Leon Finkbiner, and Christopher DeKruif.

80 The cases in this study that involve social media manipulation include those of: Joseph J. Ostrowski, Brian Newman, Jonathan Wryn Vance, James Allen, Jeremy Brendan Sears, Patrick Connolly, Lucas Michael Chansler, Jared James Abrahams, Nicholas Joseph Rotundo, Mario Lebron-Caceres, Cameron Wiley, Plony (John Doe), Joseph Simone, Joshua Blankenship, Mark Robert Reynolds, Marc Joseph Punzalan, Bryan Jacobs, Austin Williams, Michael Macaluso, Joshua James Geer, Tremain Hutchinson, Ralph Daniel Smith, Anton Martynenko, Cesar Mauricio Estrada-Davila, Jarrod James Williams, Eduardo Arturo Romero Barrios, Russell Freed, Michael Martinez, Christopher Patrick Gunn, Denis Aguilar, Jordan James Kirby, Lucas Robinson, Gerardo Diaz-Chavez, Bryan Harris, Anthony Stancl, Jesus Javier Hernandez Carvajal, James F. Connor V, Gregory Kasarcik, Jason Betensky, Theodore J. Castine, Corey Gallisdorfer, Jesse S. Williams, Cameron Scot Bivins-Breeden, Jorge Juan Perez, Dustin Coleman, Trevor Shea, Gregory Bogomol, Patrick Killen, Brian Caputo, Daniel Dunfee, Miguel Angel Moran, Nicholas Kurtz, Nicholas Glenn Wilcox, Melvin Barber Bridgers III, Aydin Coban, Cody Lee Jackson, Christopher DeKruif, William T. Koch, Wesley Brandt, Kai Lundstroem Pedersen, Daniel Chase Harris, Jimmy Caraballo-Colon, Matthew C. Walker, Chase Coston, and Richard Leon Finkbiner.

81 The cases in this study that involve minors and a form of social media manipulation include those of: Brian Newman, Jeremy Brendan Sears, Patrick Connolly, Lucas Michael Chansler, Cameron Wiley, Plony (John Doe), Joseph Simone, Joshua Blankenship, Mark Robert Reynolds, Marc Joseph Punzalan, Bryan Jacobs, Austin Williams, Michael Macaluso, Joshua James Geer, Tremain Hutchinson, Ralph Daniel Smith, Anton Martynenko, Cesar Mauricio Estrada-Davila, Jarrod James Williams, Eduardo Arturo Romero Barrios, Christopher Patrick Gunn, Denis Aguilar, Jordan James Kirby, Lucas Robinson, Gerardo Diaz-Chavez, Bryan Harris, Jesus Javier Hernandez Carvajal, Gregory Kasarcik, Jason Betensky, Theodore J. Castine, Corey Gallisdorfer, Jesse S. Williams, Cameron Scot Bivins-Breeden, Jorge Juan Perez, Dustin Coleman, Trevor Shea, Gregory Bogomol, Patrick Killen, Brian Caputo, Daniel Dunfee, Miguel Angel Moran, Nicholas Kurtz, Nicholas Glenn Wilcox, Cody Lee Jackson, William T. Koch, Wesley Brandt, Kai Lundstroem Pedersen, Daniel Chase Harris, Jimmy Caraballo-Colon, Matthew C. Walker, and Chase Coston.

82 The cases in this study that involve adult victims and catfishing include those of: Nicholas Joseph Rotundo, Mario Lebron-Caceres, James F. Connor V.

83 The cases in this study that involved adults and some form of computer hacking include those of: Karen Kazaryan, Sungkook Kim, Adam Paul Savader, Luis Mijangos, Michael Ford, Ivory Dickerson, Joseph J. Ostrowski, Jonathan Wryn Vance, James Allen, and Jared James Abrahams.

84 The cases in this study that involved minor victims and computer hacking are: Ryan J. Vallee, Brian Newman, Jeremy Brendan Sears, Patrick Connolly, and Lucas Michael Chansler.

85 The cases in this study that involved computer hacking are: Karen Kazaryan, Ryan J. Vallee, Sungkook Kim, Adam Paul Savader, Luis Mijangos, Michael Ford, Ivory Dickerson, Joseph J. Ostrowski, Brian Newman, Jonathan Wryn Vance, James Allen, Jeremy Brendan Sears, Patrick Connolly, Lucas Michael Chansler, and Jared James Abrahams.

86 *See* United States v. Joseph Ostrowski, No. 12-00131-EMK (M.D. Penn).

87 *See* United States v. Dustin Coleman, No. 14-00004-RRE (D. N.D.).

88 *See* United States v. Jason Betensky, No. 11-00015-CFD (D. Conn).

89 Complaint, United States v. Adam Paul Savader, No. 2:13-cr-20522 (E.D. Mich. Apr. 17, 2013).

90 The cases in this study that included significant interstate elements are those of: Luis Mijangos, Adam Paul Savader, Ivory Dickerson, Michael Ford, James Allen, Jonathan Wryn Vance, Brian Newman, Joseph J. Ostrowski, Jeremy Brendan Sears, Patrick Connolly, Jared James Abrahams, Lucas Michael Chansler, John Bryan Villegas, Destin Whitmore, Christopher Steibing, John Michael Fowler, Christopher Patrick Gunn, Dustin Coleman, Aydin Coban, Patrick Killen, James F. Connor V, Gregory Kasarcik, Miguel Angel Moran, Theodore J. Castine, Jesse S. Williams, Jarrod James Williams, Joshua James Geer, Melvin Barber Bridgers III, Corey Gallisdorfer, Jorge Juan Perez, Brian Caputo, Gregory Bogomol, Cameron Scot Bivins-Breeden, Jason Betensky, Eduardo Arturo Romero Barrios, Nicholas Kurtz, Daniel Dunfee, Trevor Shea, Nicholas Glenn Wilcox, Cody Lee Jackson, Christopher DeKruif, Wesley Brandt, William T. Koch, Chase Coston, Kai Lundstroem Pedersen, Daniel Chase Harris, Matthew C. Walker, Richard Leon Finkbiner, and Jimmy Caraballo-Colon.

91 The following cases had involved more than ten jurisdictions: Michael Ford, Christopher Patrick Gunn, Nicholas Glenn Wilcox, Richard Leon Finkbiner, Jimmy Caraballo-Colon, and Lucas Michael Chansler.

92 The cases in this study involving five or more jurisdictions included those of: Jared James Abrahams, Eduardo Arturo Romero Barrios, Patrick Connolly, Daniel Dunfee, Nicholas Kurtz, Trevor Shea, and Michael Ford.

93 The cases in this study that involve a perpetrator victimizing an individual in a country other than that in which the perpetrator resides include those of: Jesus Javier Hernandez Carvajal, Ivory Dickerson, John Michael Fowler, William T. Koch, Wesley Brandt, Kai Lundstroem Pedersen, Daniel Chase Harris, Chase Coston, Jeremy Brendan Sears, Matthew C. Walker, Patrick Connolly, Jared James Abrahams, Michael Ford, Richard Leon Finkbiner, Jimmy Caraballo-Colon, and Lucas Michael Chansler.

94 The following cases involved demands for actual in-person sexual activity: Garrett Drew Roegner, Denis Aguilar, Jordan James Kirby, Lucas Robinson, Gerardo Diaz-Chavez, Bryan Harris, Anthony Stancl, Jesus Javier Hernandez Carvajal, Cody Lee Jackson, John Michael Fowler, Christopher DeKruif, William T. Koch, and Wesley Brandt.

95 *See*, e.g., United States v. Christopher Steibing, No. 14-00256-HB (E.D. Pa.).

96 *See, e.g.,* United States v. Ralph Daniel Smith, No. 15-00342-BKS-1 (N.D.N.Y.).

97 *See, e.g.,* United States v. Cody Lee Jackson, No. 15-118-MRB (S.D. Ohio).

98 Complaint, United States v. Brian Caputo, No. 14-00041-LJO (E.D. Calif) at 5–6.

99 Government's Sentencing Memorandum, United States v. Richard L. Finkbiner, Nos. 12-0021-WTL-CMM, 13-0002-WTL-CMM (S.D. Ind.) at 2.

100 We are indebted to Elishe Julian Wittes for helping develop these assumptions and the resulting estimates.

101 Federal Bureau of Investigation, *Sextortion of Children in the United States: A Fact Sheet for Parents and Children* (July 2015), https://www.fbi.gov/news/stories/2015/july/sextortion/stop-sextortion-brochure.

102 The cases in this study that were prosecuted under 18 USC § 2251 include those of: Theodore J. Castine, Trevor Shea, Gregory Bogomol, Jesse S. Williams, Brian Caputo, Jimmy Caraballo-Colon, Melvin Barber Bridgers III, Russell Freed, Anton Martynenko, Ralph Daniel Smith, Ivory Dickerson, Christopher DeKruif, Bryan Jacobs, Michael Martinez, Michael Macaluso, James Allen, Christopher Steibing, Jordan James Kirby, Corey Gallisdorfer, Cameron Scot Bivins-Breeden, Cody Lee Jackson, Joshua James Geer, Daniel Chase Harris, Austin Williams, Tremain Hutchinson, Christopher, Patrick Gunn, Joshua Blankenship, Marc Joseph Punzalan, Patrick Connolly, Kai Lundstroem Pedersen, Patrick Killen, Lucas Michael Chansler, Richard Leon Finkbiner, Jeremy Brendan Sears, Matthew C. Walker, Brian Newman, Lucas Robinson, William T. Koch, Dustin Coleman, Joseph J. Ostrowski, Nicholas Glenn Wilcox, Jonathan Wryn Vance, and Wesley Brandt.

103 18 USC § 2251(a).

104 The cases in this study prosecuted under 18 USC § 2252 include those of: Jesse S. Williams, Brian Caputo, Jimmy Caraballo-Colon, Melvin Barber Bridgers III, Russell Freed, Anton Martynenko, Christopher DeKruif, Bryan Jacobs, Michael Martinez, Joshua James Geer, Daniel Chase Harris, Austin Williams, Tremain Hutchinson, Mark Robert Reynolds, Kai Lundstroem Pedersen, Patrick Killen, Lucas Michael Chansler, Richard Leon Finkbiner, Matthew C. Walker, Brian Newman, Lucas Robinson, William T. Koch, Dustin Coleman, Wesley Brandt, Jesus Javier Hernandez Carvajal, Sungkook Kim, Destin Whitmore, and John Michael Fowler.

105 The cases in this study prosecuted under 18 USC § 2252A are: Ralph Daniel Smith, Ivory Dickerson, Christopher DeKruif, Bryan Jacobs, Michael Martinez, Michael Macaluso, Tremain Hutchinson, Mark Robert Reynolds, Jorge Juan Perez, Christopher Patrick Gunn, Jeremy Brendan Sears, Matthew C. Walker, Brian Newman, Lucas Robinson, William T. Koch, Dustin Coleman, and Garrett Drew Roegner.

106 The cases in this study prosecuted under 18 USC § 2422(b) include those of: Michael Macaluso, Joshua James Geer, Daniel Chase Harris, Austin Williams, Tremain Hutchinson, Christopher Steibing, Nicholas Kurtz, Jorge Juan Perez, Jordan James Kirby, Corey Gallisdorfer, Jason Betensky, Cameron Scot Bivins-Breeden, Cody Lee Jackson, Bryan Harris, Wesley Brandt, Destin Whitmore, Nicholas Glenn Wilcox, Jonathan Wryn Vance, and John Michael Fowler.

107 State of Rhode Island v. Joseph Simone, No. P2-2012-0684A (Providence County Superior Court). *See also* W. Zachary Malinowski, *Former Moses Brown Wrestling Coach Sentenced for Child Pornography, Indecent Solicitation*

of Minor and Extortion, Providence Journal (Dec. 12, 2014), http://www.providencejournal.com/article/20141212/NEWS/312129915.

108 State v. Cameron Wiley, No. 2014ML023981 (Cir. Ct. Milwaukee County).

109 Complaint, United States v. Jared James Abrahams, No. 8:13-mj-00422 (C.D. Cal. Sep. 17, 2013) at 20. Note: We are identifying Ms. Wolf in this report only because she chose to speak publicly about the incident. As a general matter, we are not identifying sextortion victims even when their identities are readily discernible from court papers.

110 Evan Perez, Shimon Prokupecz and Tom Cohen, *More than 90 People Nabbed in Global Hacker Crackdown,* CNN (May 19, 2014), http://www.cnn.com/2014/05/19/justice/us-global-hacker-crackdown/index.html. See also Complaint, *supra* note 108, at 20.

111 *Id.* at 7–8.

112 *Id.* at 19. See also Plea Agreement at 10, United States v. Jared James Abrahams, No. 8:13-cr-00199 ((C.D. Cal. Nov. 11, 2013); Government Sentencing Position at 1, United States v. Jared James Abrahams, No. 8:13-cr-00199 (C.D. Cal. February 17, 2014).

113 Complaint, *supra* note 108, at 10–11.

114 *Id.* at 10, 20–21.

115 *Id.* at 9–10.

116 *Id.* at 19.

117 *Id.* at 8–9.

118 *Id.* 10–12.

119 *Id.* 1–-12.

120 Plea Agreement, *supra* note 111.

121 Judgment, United States v. Jared James Abrahams, No. 8:13-cr-00199 (C.D. Cal. Mar. 21, 2014).

122 *Sextortion: Help Us Locate Victims of an Online Predator* (July 7, 2015), https://www.fbi.gov/news/stories/2015/july/sextortion.

123 *Special Agent Discusses Sextortion Case* (July 7, 2015), https://www.fbi.gov/news/stories/2015/july/sextortion/video/special-agent-discusses-sextortion-case.

124 Indictment at 2, United States v. Lucas Michael Chansler, No. 3:10-cr-00100 (M. D. Fla. Apr. 15, 2010).

125 *Id.* 2–3

126 *Special Agent Discusses Sextortion Case, supra* note 122*; see also* Brad Stone, *Accuser Says Web Site for Teenagers has X-Rated Link,* New York Times (July 11, 2007), http://nyti.ms/20eQQMo.

127 Indictment, *supra* note 123, at 2–3.

128 *Victim of Sextortion Speaks Out* (July 7, 2015), https://www.fbi.gov/news/stories/2015/july/sextortion/video/victim-of-sextortion-speaks-out.

129 *Special Agent Discusses Sextortion Case, supra* note 122.

130 Indictment, *supra* note 123.

131 Plea Agreement at 1, United States v. Lucas Michael Chansler, No. 3:10-cr-00100 (M. D. Fla. Apr. 15, 2010). See also Judgment at 2, United States v. Lucas Michael Chansler, No. 3:10-cr-00100 (M. D. Fla. Nov. 13, 2014).

132 *Sextortion of Children in the United States: A Fact Sheet for Parents and Children* (July 2015), https://www.fbi.gov/news/stories/2015/july/sextortion/stop-sextortion-brochure. In our dataset, Connolly is classified as only having seven identified victims and, at least in the court papers we reviewed, there was not a high-end estimate above that. Dickerson, by contrast, is listed as having four identified victims, but in his case, prosecutors estimated "more than 100" total victims.

133 Amy L. Edwards, *Judge Calls Child Exploiter a 'Narcissistic Demon,' Hands Down 30-year Sentence,* Orlando Sentinel (June 18, 2010), http://articles.orlandosentinel.com/2010-06-18/news/os-orlando-child-exploitation-20100618_1_sentence-patrick-connolly-victims-lives.

134 Criminal Complaint at 14, 31, United States v. Patrick Connolly, No. 6:09-mj-01069 (M.D. Fla. Mar. 13, 2009).

135 Plea Agreement at 18, United States v. Ivory Dickerson, No. 6:07-cr-00150 (M.D. Fla. Sept. 13, 2007).

136 *Cyber Alerts for Parents & Kids: Tip #2: Beware of "Sextortion"* (Feb. 10, 2012), https://www.fbi.gov/news/stories/2012/february/sextortion_021012.

137 Plea Agreement at 19, *supra* note 134.

138 Criminal Complaint at 11, United States v. Ivory Dickerson, No. 6:06-cr-00238 (M.D. Fla. Dec. 1, 2006).

139 *Id.* at 16–17.

140 *Id.* at 28–29; *see* also Plea Agreement, *supra* note 134, at 17–18.

141 Plea Agreement, *supra* note 134, at 22.

142 Criminal Complaint, *supra* note 133, at 31.

143 Judgment at 1, United States v. Ivory Dickerson, No. 6:06-cr-00238-A (M.D. Fla. Nov. 30, 2007). Plea agreement, *supra* note 134, at 1.

144 Superseding Indictment, United States v. Patrick Connolly, No. 6:09-cr-00047 (M.D. Fla. May 20, 2009).

145 Plea Agreement, United States v. Patrick Connolly, No. 6:09-cr-00047 (M.D. Fla. Jan. 8, 2010).

146 Amy L. Edwards, *supra* note 132.

147 Affidavit in Support of a Criminal Complaint and Arrest Warrant at 4, United States v. Michael C. Ford, No. 1:15-cr-00319 (N.D. Ga. May 15, 2015).

148 *Id.* at 10–16

149 *Id.* at 13–15

150 *Id.* at 16.

151 Indictment at 1–2, United States v. Michael C. Ford, No. 1:15-cr-00319 (N.D. Ga. Aug. 18, 2015).

152 Affidavit, *supra* note 146, at 15.

153 Indictment, *supra* note 150, at 12–13.

154 *Id.* at 4.

155 *Id.* at 13.

156 *Id.* at 3, 6, 9, 10.

157 *Id.* at 15.

158 *Id.* at 3, 7–8.

159 Kate Brumback, *"Sextortion" Scheme: US Embassy Worker Faces up to 8 Years in Prison*, Associated Press (Mar. 21, 2016), http://www.csmonitor.com/USA/Justice/2016/0321/Sextortion-scheme-US-Embassy-worker-faces-up-to-eight-years-in-prison/.

160 Indictment, *supra* note 150, at 4. *See also* Press Release, Dpt. of Justice, Former U.S. State Department Employee Pleads Guilty to Extensive Computer Hacking, Cyberstalking, and "Sextortion" Scheme (Dec. 9, 2015), http://www.justice.gov/opa/pr/former-us-state-department-employee-pleads-guilty-extensive-computer-hacking-cyberstalking.

161 Indictment, *supra* note 150, at 17–21.

162 Guilty Plea and Plea Agreement at 1–2, United States v. Michael C. Ford, No. 1:15-cr-00319 (N.D. Ga. Dec. 9, 2015).

163 Judgment, United States v. Michael C. Ford, No. 1:15-cr-00319 (N.D. Ga. Mar. 22, 2016).

164 Superseding Indictment at 1, United States v. Christopher Patrick Gunn, 2:12-cr-00064 (M.D. Ala. Jun. 6, 2012).

165 *Id.* at 1–2.

166 The Omegle web site notes, "Predators have been known to use Omegle, so please be careful." It also includes a disclaimer that reads partially, "Understand that human behavior is fundamentally uncontrollable, that the people you encounter on Omegle may not behave appropriately, and that they are solely responsible for their own behavior. Use Omegle at your own peril." *Omegle: Talk to Strangers!* (last accessed Apr. 23, 2016), http://www.omegle.com/.

167 Indictment, *supra* note 163, at 3.

168 Allie Conti, *How a "Sextortionist" Went from Trolling Bieber Fan Pages to Being Sent to Prison for Child Pornography,* Vice (Jun. 3, 2015), http://www.vice.com/read/how-a-sextortionist-went-from-trolling-bieber-fan-pages-to-being-sent-to-prison-for-child-pornography-603. See also First Superseding Indictment at 4, United States v. Jeremy Brendan Sears, No. 2:14-cr-00274 (C.D. Cal. Jun. 10, 2015); Criminal Complaint at 3, 14, United States v. Jeremy Brendan Sears, No. 2:14-cr-00274 (C.D. Cal. Apr. 29, 2015).

169 Criminal Complaint, *supra* note 167, at 5.

170 Conti, *supra* note 167.

171 Indictment, *supra* note 167, at 2–7.

172 Complaint, *supra* note 167, at 12.

173 Plea Agreement, United States v. Christopher Patrick Gunn, No. 2:12-cr-00064 (M.D. Ala. Aug. 23, 2012).

174 Judgment, United States v. Christopher Patrick Gunn, No. 2:12-cr-00064 (M.D. Ala. Jan. 29, 2013).

175 In contrast to both the initial judgment and a later amended judgment, Gunn's plea agreement lists him as having pleaded guilty to two counts of producing child pornography, 15 counts of extortion, and seven counts of stalking—an additional ten counts to those listed in the judgment. The Department of Justice's press release on Gunn's sentencing also lists these additional charges. The cause of this discrepancy is unclear. See Plea Agreement, *supra* note 172; Amended Judgment, United States v. Christopher Patrick Gunn, No. 2:12-cr-00064 (M.D. Ala. Jan. 29, 2013); Press Release, Dep't. of Justice, Child Predator is Sentenced to 35 Years in Prison for His Massive Online Sextortion Scheme, (Jan. 2013), https://www.justice.gov/usao-mdal/pr/child-predator-sentenced-35-years-prison-his-massive-online-sextortion-scheme.

176 Judgment, United States v. Jeremy Brendan Sears, No. 2:14-cr-00274 (C.D. Cal. May 29, 2015).

177 Plea Agreement, United States v. Jeremy Brendan Sears, No. 2:14-cr-00274 (C.D. Cal. Dec. 14, 2014).

178 Indictment, *supra* note 167.

179 Government's Sentencing Memorandum at 3–4, United States v. Richard Leon Finkbiner, No. 2:12-cr-00021 (S.D. Ind. June 18, 2013).

180 Criminal Complaint at 7, United States v. Richard Leon Finkbiner, No. 2:12-cr-00021 (S.D. Ind. Apr. 6, 2012).

181 Sentencing Memorandum, *supra* note 178, at 2–3.

182 *Id.* at 3.

183 *Id.* at 8.

184 *Id.* at 11.

185 *Id.* at 9.

186 *Id.* at 5–7.

187 *Id.* at 2.

188 Plea Agreement at 1, United States v. Richard Leon Finkbiner, No. 2:12-cr-00021 (S.D. Ind. Jan. 30, 2013).

189 *Id.*

190 Judgment, United States v. Richard Leon Finkbiner, No. 2:12-cr-00021 (S.D. Ind. July 2, 2013).

191 Kevin Robillard, *Ex-Romney Intern Arrested,* Politico (Apr. 24, 2014), http://www.politico.com/story/2013/04/ex-romney-intern-arrested-blackmail-090552.

192 Information, United States v. Adam Paul Savader, No. 2:13-cr-20522 (E.D. Mich. July 15, 2013).

193 Government's Sentencing Memorandum at 4, United States v. Adam Paul Savader, No. 2:13-cr-20522 (E.D. Mich. Apr. 29, 2014).

194 Criminal Complaint at 9, United States v. Adam Paul Savader, No. 2:13-cr-20522 (E.D. Mich. Apr. 17, 2013).

195 *Id.* at 7; *see also* Sentencing Memorandum, *supra* note 192, at 22.

196 *Id.* at 7.

197 *Id.* at 4.

198 *Id.*

199 *Id.* at 3–4.

200 *See Send All Calls to Voicemail* (last accessed Apr. 23, 2016), https://support.google.com/voice/answer/115106?hl=en.

201 Complaint, *supra* note 193, at 2.

202 *Id.* at 5, 12.

203 *Id.* at 5–6.

204 Judgment, United States v. Adam Paul Savader, No. 2:13-cr-20522 (E.D. Mich. Apr. 29, 2014).

205 Plea Agreement, United States v. Adam Paul Savader, No. 2:13-cr-20522 (E.D. Mich. Nov. 14, 2013).

206 Information, *supra* note 191.

207 Carrie Levine, *Can This Man Buy an Election from Jail?,* The Daily Beast (June 30, 2015), http://www.thedailybeast.com/articles/2015/06/30/can-this-man-buy-an-election-from-jail.html.

208 Crim. App. 2656/13, Plony (John Doe) v. The State of Israel, delivered on January 21, 2014. http://elyon1.court.gov.il/files/13/560/026/z03/13026560.z03.htm

209 *Victim of Sextortion Speaks Out* (July 7, 2015), https://www.fbi.gov/news/stories/2015/july/sextortion/video/victim-of-sextortion-speaks-out

210 *Sextortion: Help Us Locate Victims of an Online Predator* (July 7. 2015), https://www.fbi.gov/news/stories/2015/july/sextortion.

211 Peter Holly, *The Man who Posed as his Daughter's Online Boyfriend to Get Nude Photos of Her*, Washington Post (Mar. 17 2016), https://www.washingtonpost.com/news/true-crime/wp/2016/03/17/the-man-who-posed-as-his-daughters-online-boyfriend-to-get-nude-photos-of-her/.

212 Liz Brody, *Meet Ashley Reynolds, the Woman Fighting "Sextortion,"* Glamour (July 7 2015), http://www.glamour.com/inspired/2015/07/ashley-reynolds-the-woman-fighting-sextortion.

213 *Id.*

214 Jesse Paul, *Ohio Man Sentenced in Jefferson County for Sexually Exploiting Teen*, Denver Post (Jan, 12, 2015), http://www.denverpost.com/news/ci_27306114/ohio-man-sentenced-jefferson-county-sexually-exploiting-teen.

215 David Kushner, *The Hacker is Watching*, GQ Magazine (Jan. 11 2012), http://www.gq.com/story/luis-mijangos-hacker-webcam-virus-internet.

216 Criminal Minutes at 4, United States v. Jared James Abrahams, No. 8:13-cr-00199 (Mar. 17, 2014).

217 Sentencing Minutes (Excerpts) at 44, 46, United States v. Lucas Michael Chansler, No. 3:10-cr-00100 (Mar. 12, 2015).

218 *Id.* at 49.

219 *Id.* at 28.

220 Exhibit B, Victim Impact Statement at 1, United States v. Adam Paul Savader, No. 2:13-cr-20522 (Apr. 16, 2014), quoted in Government's Sentencing Memorandum at 13-14, United States v. Adam Paul Savader, No. 2:13-cr-20522 (Apr. 16, 2014). This should be: Government's Sentencing Memorandum at 13–14, United States v. Adam Paul Savader, No. 2:13-cr-20522 (Apr. 16, 2014) (*citing* Exhibit B, Victim Impact Statement at 1, United States v. Adam Paul Savader, No. 2:13-cr-20522 (Apr. 16, 2014)).

221 Exhibit A, Victim Impact Statement at 1, United States v. Adam Paul Savader, No. 2:13-cr-20522 (Apr. 16, 2014), quoted in Government's Sentencing Memorandum at 13-14, United States v. Adam Paul Savader, No. 2:13-cr-20522 (Apr. 16, 2014). Should be be: Government's Sentencing Memorandum at 13–14, United States v. Adam Paul Savader, No. 2:13-cr-20522 (Apr. 16, 2014) (*citing* Exhibit A, Victim Impact Statement at 1, United States v. Adam Paul Savader, No. 2:13-cr-20522 (Apr. 16, 2014)).

222 Transcript of Sentencing at 29, *United States v. Ivory Dickerson*, No. 6:06-cr-00238 (Aug. 20, 2008).

223 *Id.* at 31.

224 *Id.* at 32–33.

225 Government's Sentencing Memorandum at 4–6, United States v. Richard L. Finkbiner, No. 2:12-cr-00021 (June 18, 2013).

226 Dep't. of Justice, Fact Sheet: Project Safe Childhood (Feb. 21, 2012), https://www.justice.gov/psc/file/842426/download.

GOVERNANCE STUDIES

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
brookings.edu/governance

EDITING
Elizabeth Sablich

PRODUCTION & LAYOUT
Nick McClellan

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU

Support for this publication was generously provided by the Digital Trust Foundation.