DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 32 | Issue 1 Article 1

Strategies to Deter Child Pornography in the Absence of a Mandatory Encryption Back Door: Tipster Programs, A Licensed Researcher System, Compelled Password Production, & Private Surveillance

Anthony Volini
DePaul University, avolini@depaul.edu

Farzana Ahmed
DePaul University College of Law, fahmed24@depaul.edu

STRATEGIES TO DETER CHILD PORNOGRAPHY IN THE ABSENCE OF A MANDATORY ENCRYPTION BACK DOOR: TIPSTER PROGRAMS, A LICENSED RESEARCHER SYSTEM, COMPELLED PASSWORD PRODUCTION, & PRIVATE SURVEILLANCE

*Anthony G. Volini**

&

*Farzana Ahmed***

INTRODUCTION

Online child pornography (CP) is a serious issue. For several decades, law enforcement has requested a mandatory encryption back door, referencing child pornography as the key motivation. Given that law enforcement may never have such a back door based on privacy concerns, the question arises of what can be done to deter CP. Given the absence of a mandatory encryption back door, the FBI in 2021 worked with a private company that sold encrypted devices to hundreds of organized crime syndicates, resulting in 800 arrests in 16 countries (as the FBI had the ability to decrypt). While this was a creative strategy, other strategies for detecting child pornography are explored in this article given that law enforcement's decades-long push for a mandatory encryption back door may continue to be outweighed by privacy interests. Potential strategies addressed include a conventional tipster program, an anonymous tipster program, a licensed private researcher system to corroborate law enforcement claims, scanning by private tech companies for CP content, and brief exploration of a narrow Fifth Amendment exception to compelled password production (which might fail constitutional muster).

OVERVIEW

To deter child pornography[1], we propose a conventional tipster reward system for reporting of preteen child pornography

* Senior Professional Lecturer at DePaul University College of Law, Registered Patent Attorney, M.S. Cybersecurity (Networking & Infrastructure), Certified

(CP), exploration of an alternative anonymous reward system (but raising the concern of swatting), licensing of private researchers to corroborate law enforcement claims about the extent and types of CP in society, and a CP tax to support both reward payments and hiring of additional law enforcement investigators. We further observe the possible growth of private surveillance by tech platforms to assist in CP detection, and we discuss private party scanning from both a technological standpoint and with regard to legal and policy considerations.

Regarding either an identified witness system or anonymous reward system, an innocent person who encounters CP generally has two options to avoid a criminal charge upon discovering such content on her computer: (1) report to authorities or (2) delete the content immediately. Given that some individuals may be reluctant to report, providing an award system, either transparent or anonymous, may stimulate increased reporting. In any reward system, care must be taken to avoid a Cobra Effect of rewards having the unintended consequence of increasing rather than reducing online CP. Therefore, at a minimum, any system should

---

Information Privacy Professional/United States (CIPP/US), CIPP/Europe (CIPP/E), Cybersecurity Fundamentals Certificate (CSXF).

** Farzana Ahmed is a 2022 DePaul University College of Law J.D. Candidate. Farzana is the Editor-in-Chief for the DePaul Journal of Art, Technology, and Intellectual Property Law. At DePaul University College of Law, she is pursuing both the Information Technology, Cybersecurity, and Data Privacy Law certificate and Tax Law certificate. Farzana is a member of the International Association of Privacy Professionals and is pursuing privacy certifications. The authors also thank Ethan Perbohner, a 2022 DePaul University College of Law J.D. Candidate, for contributing research insights on compelled password production below.

[1] This article is dedicated to the memory of my father, Thomas Anthony Volini, Esq. (1945-2021), who has enthusiastically supported all of my research and writing aimed at the betterment of society. It is further dedicated to Christopher Meyer, Tara Sue Huffman, and all other children who have been victims of sexual or other abuse. It is further dedicated in memory of federal agents Daniel Alfin and Laura Schwartzenberger who died attempting to execute a search warrant in a case involving suspected child pornography. *See* https://www.cnn.com/2021/02/08/us/fbi-agents-rarely-killed-in-shootings-trnd/index.html.

require a conviction of a suspect as a condition for payment of the award.

This article proposes that any reward system could prioritize preteen victims (i.e., victims twelve and younger) as this category would target the most vulnerable victims and would exclude some grey area instances of self-produced CP shared between sexually active teenagers.[2] Prioritization of the most egregious crimes and enforcement efforts therefore is certainly an important goal to avoid overreach, such as mass governmental surveillance of high school students. One form of overreach may involve law enforcement scope creep (or "mission creep") where a specific type or species of crime might be used as justification for enforcement efforts against an entire genus of crime. Such an example is law enforcement might use human trafficking concern as a justification for spending massive resources on detecting and prosecuting ordinary low-level prostitution offenses. Another example could be seen in the PATRIOT Act's reduction in overall privacy in society in response to terrorism concerns.

Regarding licensing of private researchers, under current law private parties are generally restricted in that research of illicit sites could lead to intentional possession of illegal content. Thus, society is generally reliant on law enforcement's narrative. So, there is a theoretical risk of fear mongering or exaggeration that exists with respect to that narrative regarding lobbying for legislation or funding. Accordingly, private party corroboration of law enforcement's claims as to the scope of the problem may counteract suspicion of fear mongering as to proposed legislation or budget requests. Providing academics and legislators with information from independent researchers should in theory assist in development of informed opinions on the issues. This article does not accuse law enforcement of fear mongering tactics in the CP space, but it does highlight this as a theoretical risk given historical

[2] Granted, abuse of teenagers by adults is still a serious issue, but we suggest that rewards substantially focus on the most egregious crimes.

accounts of alleged fear mongering with respect to the war on drugs and other situations.

While a private licensed bounty hunter system is considered, it may be too problematic from an evidentiary standpoint to make it feasible (e.g., defense attorneys questioning a bounty hunter's financial motives and tactics). However, further exploration should not be ruled out, especially given the possibility that IT platforms could potentially create innovative crowdsourced methods to identify and deter illegal online content.

This article also suggests the possibility that the U.S. Supreme Court should consider allowing compelled production of passwords/decryption keys in CP cases (treating them like physical keys), and penalizing failure to produce the keys, given the concern that warrant-proof encryption platforms may facilitate widespread distribution of undetectable CP. However, the authors are uncertain how the Court may conclude on this divisive issue.

Regarding a CP tax, a fairness argument is that large tech companies providing warrant proof encryption platforms should strive to counteract the problem, particularly where they are deriving large revenue from platforms abused by criminals. Thus, a modest tax seems fair to increase law enforcement funding in this area given law enforcement's position that CP arrests represent only the tip of the iceberg in terms of criminal activity in this area. (Additionally or alternatively, a charitable contribution mechanism or tax credit could be established for any reward system.)

In 2021, discussion arose regarding Apple's plan to scan its devices for perceptual hash matches. To deepen the technological understanding, this article discusses the difference between cryptographic hashes and perceptual hashes. Further it discusses possible issues raised by such scanning such as false positive hash collisions and concern over law enforcement scope creep. Regarding legal concerns, the private search doctrine is also briefly discussed. In the absence of a mandatory back door, tech platforms should continue to explore tech solutions to detect only the most

serious crimes, striking a suitable balance between privacy and protecting society (e.g., law enforcement and tech platforms might acquiesce to no detection of a variety of low-level criminal activity to support overall privacy in society).

This article also discusses how the FBI and some private parties advocate backdoors and a warrant requirement safeguard. However, the possibility of abuse is discussed, including potential scope or mission creep where law enforcement could take advantage of newly gained powers for uses beyond the original purpose.

CONTENTS

I. Privacy Advocates Favor Strong Warrant Proof Encryption While Law Enforcement Desires a "Front Door"[3]

Tension exists between privacy advocates and law enforcement regarding whether private tech platforms should be compelled to provide a back door to their encryption technologies. The following sections discuss the important factors and considerations for either side. Ultimately, this article concludes that law enforcement will continue to fail in its quest for mandatory decryption. Thus, Part II of this article addresses what might be done to improve detection and prevention of CP.

A. Arguments for a Front Door

For many decades law enforcement has long argued for a mandatory front door to lawfully tackle CP.[4] However, this desire has been outweighed by privacy and security concerns.[5] CP is a crime which affects the most vulnerable members of society and tends to have lasting effects on the victims that current court resolutions do not address. Existing regulations and resolutions barely begin to create a sufficient legal infrastructure that can protect society from the dangers of continued CP activity with the proliferation of the Internet; thus, law enforcement continues its

[3] Portions, particularly of Part I herein, are copied directly from Volini's prior work: Anthony Volini, *A Deep Dive into Technical Encryption Concepts to Better Understand Cybersecurity & Data Privacy Legal & Policy Issues*, 28 J. INTELL. PROP. L. 291 (2021). Available at: https://digitalcommons.law.uga.edu/jipl/vol28/iss2/2. This content is reprinted with the permission of the [University of Georgia] *Journal of Intellectual Property Law* from Vol. 28, No. 2 (2020-2021).

[4] As discussed in Part II below, Congress is contemplating a bill called the Lawful Access to Encrypted Data. This bill would require tech companies to put backdoors in their products to allow law enforcement access to customer's data with a warrant.

[5] Swire, Peter and Ahmad, Kenesa*, Encryption and Globalization* (November 16, 2011). COLUM. SCI. L. REV., Vol. 23, 2012, Ohio State Public Law Working Paper No. 157, Available at SSRN: https://ssrn.com/abstract=1960602 or http://dx.doi.org/10.2139/ssrn.1960602 (noting at page 416 that "[i]n 1999, . . . the administration shifted position to allow largely unrestricted export of encryption technologies. Encryption law and policy discussions largely faded from view.").

push for a back door. Certainly, bad actors would be inhibited from downloading and sharing CP if law enforcement had an easy means to discover such activity.

1. Law Enforcement's Push for a Front Door is Conceptually a Push to Expand Access to Data Not Accessible Under CALEA

For decades, society has debated whether federal law enforcement should be provided a "back door" (now called a front door) to encryption products provided by tech companies, such as Apple's iPhone Data Protection technology.[6] Law enforcement was successful in lobbying for a front door with respect to wiretap orders under CALEA (Communications Assistance for Law Enforcement Act), which applies to telecommunications carriers, including providers of telephone service, Broadband Internet Service, and providers of VoIP.[7] Under CALEA, providers are required to modify and design their technologies with sufficient capabilities to assist and comply with such orders. So, law enforcement has historically pushed for a front door to aid their duties and work in situations of particular national concern or societal danger that traditional avenues of investigation would not suffice. Law enforcement's current push is for a larger front to encompass other technologies not reached by CALEA, such as smartphone devices or cloud providers (e.g., Dropbox or encrypted WhatsApp messages).[8]

As part of this push, FBI Director Christopher Wray raised concerns in an October 2019 speech over warrant-proof, end-to-end encryption and disclosed that it wants a "front door" to lawfully access communications with a warrant from a neutral judge upon

[6] Kif Leswing, *Apples Fight with Trump and the Justice Department,* CNBC (Jan. 16, 2020, 1:13 PM) https://www.cnbc.com/2020/01/16/apple-fbi-backdoor-battle-is-about-more-than-two-iphones.html.
[7] *See Communications Assistance for Law Enforcement Act,* FEDERAL COMMUNICATIONS COMMISSION, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance (last updated Oct. 20, 2020).
[8] David W. Opderbeck, *Encryption Policy and Law Enforcement in the Cloud*, 49 CONN. L. REV. 1657, 1671 (2017).

meeting Fourth Amendment requirements.[9] Similarly, in 2016 FBI Director James Comey publicly pushed for a backdoor to Apple's iPhone while seeking a court order under the All Writs Act, 28 U.S.C. § 1651, to compel Apple to unlock an encrypted iPhone 5C used by a San Bernardino attacker in 2015.[10]

Notably, both FBI Directors' concerns are based on the admirable goal of detecting terrorism and CP, but a concern exists that permitting a front door for CP may lead to subsequent scope creep into other areas. However, law enforcement has provided evidence for serious concern of society's safety that requires privacy laws to evolve with technological advancement. CALEA provided law enforcement with access to information and evidence they could not otherwise lawfully derive from the available technology before CALEA's enactment. CALEA has helped law enforcement in investigations that require more advanced tools due to the impact of technology in society. Providing a front door while limiting it to certain issues like CP may facilitate similar access to relevant information that CALEA might provide in some instances. Law enforcement would ostensibly assert that privacy laws and statutes providing law enforcement with the ability to protect society may need to once again be updated to match the available technology used in crimes and the need for access to evidence.

The desired front door would require tech companies to facilitate lawful access upon law enforcement obtaining judicial approval. Law enforcement would assert there is a pivotal need for a new larger front door to prevent and prosecute cases of child sexual exploitation and terrorism. On balance, society will likely tolerate some unsurveillable drug trafficking communications because they are low-level crimes. But with CP, law enforcement

[9] Christopher Wray*, Finding a Way Forward on Lawful Access: Bringing Child Predators Out of the Shadows,* FBI (Oct. 4, 2019), https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access.
[10] *See* Matthias Schulze, *Clipper Meets Apple v. FBI -A Comparison of the Cryptography Discourses from 1993 and 2016,* 5 COGITATIO 1 (2017) available at: https://www.cogitatiopress.com/mediaandcommunication/article/view/805; Opderbeck, *supra* note 10, at 1671 (discussing the government's usage of the All Writs Act to fill in the gap not covered by CALEA).

would argue the significant danger to the most vulnerable members of society is not likely to be tolerated. It would seem that a civilized society should not tolerate widespread undiscoverable distribution of videos and other imagery of infants and toddlers subjected to sex acts and exploitation.[11]

2. Platforms Designed for Children Should Be Accessible by Authorities

FBI Director Wray noted in his October 2019 speech that Facebook has provided more than 90% of the referrals received by the National Center for Missing & Exploited Children (NCMEC), which now receives more than 18 million referrals per year.[12] Director Wray expressed concern that if Facebook and other tech companies end up providing warrant-proof end-to-end encryption, they will willfully blind themselves to all content and eliminate the possibility of lawfully accessing particularly egregious criminal content. He notes that Facebook moving in this direction would transform Facebook "from the main provider of child exploitation tips to a dream-come-true for predators and child pornographers."[13]

Communication platforms designed exclusively for children's usage should arguably not have warrant-proof encryption. Platforms for kids should be surveillable by parents because predatory adults may try to engage children on such platforms. As companies like Facebook create new applications like

[11] A fairly horrific example is described in Olivia Solon, *Child sexual abuse images and online exploitation surge during the pandemic,* NBC NEWS (April 23, 2020, 2:01 PM) https://www.nbcnews.com/tech/tech-news/child-sexual-abuse-images-online-exploitation-surge-during-pandemic-n1190506 (where a zoom bomber delivered explicit video of a sexual assault on an infant to attendees of a virtual conference on climate change).

[12] *See Finding a Way Forward on Lawful Access: Bringing Child Predators Out of the Shadows, supra* note 11.

[13] David Shortell, *FBI director claims encryption plan would make Facebook a 'dream come true' for child pornographers,* CNN POLITICS, https://www.cnn.com/2019/10/04/politics/fbi-facebook-child-encryption/index.html (last updated Oct. 4, 2019, 3:22 PM).

Messenger for Kids or Instagram Youth[14] this warrant-proof end-to-end encryption can be a further danger to society. The goal with these new applications is to decrease the number of children under the age of 12 from lying about their age at registration to use social media and prevent targeting ads to children.[15] Facebook has said that these children accounts will be private by default for children under the age of 16 to prevent advertisers from using AI to detect children's age and target them as well as decrease the chances of suspicious accounts from finding teens.[16] However, this does not necessarily solve the issue of predators creating kid accounts to prey on children. Nor does this provide a real solution because children can change the setting to public because they want to become "viral," "TikTok famous," or some other modern "celebrity" status. These behavioral habits of the more vulnerable and less knowledgeable members of society show warrant-proof end-to-end encryption may pose a greater societal danger to children as time goes on and may create a gap in legal protection because laws and statutes have not caught up and evolved to consider these real time issues.

3. Warrant-Based Access as a Law Enforcement Tool to Combat the Use of Encryption for Nefarious Purposes

A general characterization is that the tech community generally rejects regulations, such as a mandatory back door, while policy makers are open to it. Technologists have argued that strong

[14] Facebook has paused the development of its kids platforms after pressure due to concern for children's mental health, privacy, and other human rights issues related to children. Oriana Gonzalez, *Instagram pauses development of platform for kids,* Axios Media, (Sept. 27, 2021), https://www.axios.com/instagram-pause-kids-platform-scrutiny-4f42fa4f-4dcd-411f-b44a-33ef5f18436e.html.
[15] Terry Collins, *Instagram's privacy changers: Will they actually keep creepy adults away from young users?*, USAToday (Jul. 17, 2021), https://www.usatoday.com/story/tech/2021/07/27/instagram-teen-safety-update-facebook-mark-zuckerberg/5381319001/; Samantha Murphy Kelly, *Facebook says it's moving forward with Instagram for kids despite backlash*, CNN (Jul. 27, 2021).
[16] *Id.*

encryption technologies should have no back door vulnerability built in.[17] This debate over an encryption front door will likely continue indefinitely (perhaps gaining greatest support in the wake of any significant terror attack), with legislators butting heads with the tech community.

Another argument further supporting a front door is that defendants in many jurisdictions are protected by the Fifth Amendment from being compelled to share their password with a court.[18] This situation would thus bolster law enforcement's position that certain data is indeed warrant-proof not only from a technical standpoint but also from a legal standpoint. Should the government's attempt to forensically crack a password prove impractical, the government may seek a court order compelling a defendant to disclose his password.[19]

Some courts view compelled password production as a Fifth Amendment violation, essentially viewing this as compelled self-incriminating testimony.[20] (As a side note, courts typically view

[17] *See* Schulze, *supra* note 12, at 59 (noting "[p]olicymakers in general favor strong encryption with exceptional, warrant-based access while the tech community replies that the mathematics either support secure encryption without government backdoors or exceptional access with significantly less security.").

[18] discussed in more detail below.

[19] For example, forensic crime labs may have smartphones or other devices subjected to brute force encryption for many months without success. *See Appleinsider Staff,* APPLE INSIDER, https://appleinsider.com/articles/18/04/17/researcher-estimates-graykey-can-unlock-a-6-digit-iphone-passcode-in-11 -hours-heres-how-to-protect-yourself (last visited Oct. 14, 2020) (describing how some phone passcodes can be cracked in mere hours while longer passcodes may take years to successfully brute force).

[20] *See generally* In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012) (finding that compelling defendant to decrypt his hard drive was Fifth Amendment barred), State v. Andrews, 457 N.J. Super. 14 (2018), (finding compelled production of passcodes did not violate the defendant's Fifth Amendment privilege against self-incrimination under the "foregone conclusion" exception to privilege); *But see* Pollard v. State, 287 So. 3d 649 (Fla. App. 1 Dist., 2019), (where the state's

compelled production of a physical biometric identifier, such as a fingerprint, as non-testimonial, and thus, not Fifth Amendment prohibited.[21] Therefore, if a cell phone can be unlocked by both a fingerprint and a passcode, presentation of a fingerprint to unlock the cell phone could often be compelled, but disclosure of the passcode to unlock the cell phone could not be compelled in some jurisdictions.) However, other courts may view compelled production of a password as not Fifth Amendment prohibited, relying on the foregone conclusion doctrine to justify the compelled production: i.e., the compelled production seems to fit this doctrine if the government knows the existence, possession, and authenticity of the incriminating evidence because the production involves no testimonial attribute.[22]

4. CP Seems Disturbingly Prevalent

generalized requests for multiple categories of communications, pictures, and social media activity did not describe contents of defendant's cellphone with particularity, as required to compel production of defendant's cellphone password under the foregone conclusion exception to the Fifth Amendment); *See also, e.g.*, U.S. v. Kirschner, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) (finding compelled disclosure of defendant's password would violate the Fifth Amendment:

"In this case, the government is not seeking documents or objects—it is seeking testimony from the Defendant, requiring him to divulge through his mental processes his password—that will be used to incriminate him.");

But see a contrary holding in State v. Stahl, 206 So.3d 124 (Fla. App. 2 Dist., 2016): ("requiring defendant to produce passcode did not compel defendant to communicate information that had testimonial significance."); For further discussion of cases on either side of this issue, *see* Fern L. Kletter, *Construction and Application of "Foregone Conclusion" Exception to the Fifth Amendment Privilege Against Self-Incrimination*, 25 A.L.R. Fed. 3d Art. 10 (2017).

[21] At the time of writing, courts have split on whether the compelled use of biometric authentication is permissible under the Fifth Amendment. *See* United States v. Wright, 431 F. Supp. 3d 1175, 1186-87 (D. Nev. 2020). *Compare* Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785 (D. Idaho 2019) (compelled use of a fingerprint to unlock a cellphone was not testimonial) *with* Wright, 431 F. Supp. 3d at 1187.

[22] United States v. Wright, 431 F. Supp. 3d 1175, 1186-87 (D. Nev. 2020) (finding that an officer holding a defendant's phone to their face in order to unlock the device was a violation of the defendant's Fifth Amendment rights).

One FBI news story found one website with almost 1.3 million CP images and identified 73 new victims.[23] From 2002 to 2015, NCMEC analysts located and identified 10,500 CP victims and 4.4 million reports were made to the CyberTipline.[24] These statistics show CP is not a rare crime. CP is prevalent in developed and developing nations and technology and time only make CP a more complex crime to solve. Leaders following the issue of pornography and human trafficking have said that technology has blurred the line of pornography and human trafficking (as the two activities seem interconnected).[25] The complexity of technology in its ability to hide perpetrators and mask the true nature of their actions, along with the apparent prevalence of CP, would seem to support law enforcement's continuing push for a front door.

5. Law Enforcement Would Argue that A Front Door is Needed for Detection & Prevention of Crime, i.e., the Ability to Impactfully Disrupt CP Rings and Systems, Given the Restitution to Victims is Often Unavailable or Inadequate

Some advocates are tackling whether victims can be properly compensated per normal means of justice. They propose that victims can be made whole with restitution.[26] The issue with focusing on restitution to solve child pornography is the lack of ability to right the wrongs committed against the children. There is also no way to prevent the continued circulation of the images and videos that have been taken. The best way to combat child pornography is to focus on detection and prevention.[27]

A front door would provide law enforcement with a tool to effectively begin to tackle child pornography from a detection and

[23] *The Scourge of Child Pornography*, Federal Bureau of Investigation (April 25, 2017), https://www.fbi.gov/news/stories/the-scourge-of-child-pornography.
[24] *Id.*
[25] Allison J. Luzwick*, Human Trafficking and Pornography: Using the Trafficking Victims Protection Act to Prosecute Trafficking for the Production of Internet Pornography*, 112 Nw. U. L. Rev.. 355 (2017).
[26] Cortney E. Lollar, *Child Pornography and the Restitution Revolution*, Vol. 103 J, Crim. L. & Criminology 343, 345-347 (2013).
[27] *Id.*

prevention standpoint: certainly, the ability to detect and confiscate valuable evidence that would lead to the discovery of possible victims, child exploitation rings, and perpetrators would be far more effective than relying solely on restitution efforts after the harm is committed. While the focus on restitution is crucial to helping victims in the aftermath, detection and prevention strategies are crucial to combating CP. While restitution, if available, helps the healing process, in many ways the historical focus on restitution is just a band aid for the real issue.[28] Creating a mandatory front door or reporting incentives discussed in Part II, would be helpful to combat the CP problem holistically rather than relying solely on restitution.

To elaborate on the beginnings of combating CP, finding justice for CP victims, and the restitution movement we must discuss the case that began the push for restitution, *United States v. Hesketh*.[29] The defendant in this case downloaded almost two thousand CP images of children, including those of the plaintiff, a child who had been exploited by their uncle.[30] This began the debate into whether restitution was appropriate in a non-contact case, a case where the individual has downloaded, distributed, or acted in some manner that does not involve the active physical exploitation of the child.[31] The restitution amount requested and ordered against the plaintiff's uncle was $1,125. [32] The amount of restitution the plaintiff sought in this case was $3.4 million, which many hoped would make it clear the significance of simply possessing CP, but the case was eventually settled for $130,000.[33]

After this case, there were other cases for restitution which created a divide between courts as to whether restitution is the

[28] *Id.*
[29] *Id.*
[30] *Id.*; United States v. Hesketh, No. 3:08-CR-00165 (WWE)(D. Conn. Dec. 7, 2008).
[31] Lollar, *supra* note 28.
[32] *Id.* at 345.
[33] *Id.*; Emily Bazelon, *The Price of a Stolen Childhood*, New York Times, (Jan. 24, 2013), https://www.nytimes.com/2013/01/27/magazine/how-much-can-restitution-help-victims-of-child-pornography.html.

appropriate solution.[34] Even with this movement, victims of CP do not find real peace or justice. The plaintiff in *Hesketh*, continued to pursue cases against other individuals winning more than 150 cases in courts that agreed to resolutions with restitution.[35] In many of these cases, the courts ordered recovery in small amounts, most between $7 and $1,000.[36] The plaintiff still recovered over $3 million in restitution from these additional cases.[37] Yet even with these awards, the plaintiff has still grown up haunted by their past and there is no end to the circulation of the already distributed CP. This case shows the only other attempted solutions to bring justice do not even begin to break the surface of justice nor meaningfully impact CP.

To effectively begin to tackle CP, law enforcement and courts need improvements in detection and prevention mechanisms for CP and to find points of distribution. Finding points of distribution will help find perpetrators and better achieve the goal the restitution movement aimed to accomplish: deter CP activity and help CP victims find justice. Continued distribution of CP plays an important role in why society cannot find justice for CP victims. CP will not be deterred if there are no real avenues to locating the perpetrators. CP is a serious crime that continues to affect individuals even after they have been removed from the situation because their CP images and videos can remain on websites protected by perpetrators right to privacy and continue to be circulated. Being able to access suspects' phones and computers would be the first step to effectively and meaningfully ending CP. Law enforcement needs to be able to access it to end the circulation, identify perpetrators, and identify victims who might otherwise never be discovered.

B. Arguments Against a Front Door

Various arguments against a law enforcement front (or back) door have been advanced, perhaps based on a growing distrust in society of governments (and businesses) having unfettered access

[34] *Id.*
[35] Bazelon, *supra* note 35.
[36] *Id.*
[37] *Id.*

to personal data.[38] Some key arguments against a front door include: (1) concern over law enforcement creep where the front door is established for very serious crimes or terrorism but eventually creeps into surveillance of lower-level crimes, thereby creating a police state;[39] (2) concern over any safeguards being ignored by law enforcement and a lack of law enforcement transparency with the public in terms of currently used forensics tools and their effectiveness;[40] (3) concern over a backdoor being leaked and exploited by bad actors;[41] (4) a related concern that it's technologically difficult to design breakable encryption products that are still considered to provide strong protection; (5) concern over US consumers purchasing foreign encryption products, thereby reducing sales of potentially inferior US products, thereby creating anticompetitive effects for US products;[42] (6) concern that overseas sales of US IT hardware or software may decline if a perception exists that they provide weak security on account of US

[38] *See* Ryan Budish, Herbert Burkert, & Urs Gasser, *Encryption Policy and Its International Impacts: A Framework for Understanding Extraterritorial Ripple Effects,* HOOVER INSTITUTION (2018), https://dash.harvard.edu/bitstream/handle/1/36291726/budish_webreadypdf%202.pdf?sequence=1 (noting "Apple's decision to offer end-to-end encrypted messaging and full device encryption, both enabled by default, could be seen as a direct response to declining consumer trust and concerns over NSA surveillance.")

[39] *See* Schulze, *supra* note 12, at 59 (noting "agencies might dig up cases to mandate companies to build in backdoors for more trivial reasons than fighting terrorism, a phenomenon called function creep.").

[40] *See* Ellen Nakashima, *FBI and NSA violated surveillance law or privacy rules, a federal judge found,* MSN (Sept 4. 2020), https://www.msn.com/en-us/news/us/fbi-and-nsa-violated-surveillance-law-or-privacy-rules-a-federal-judge-found/ar-BB18IVqI; *See also* Redacted, 402 F. Supp. 3d 45 (FISC 2018), finding "the FBI's querying and minimization procedures, as implemented, to be inconsistent with statutory minimization requirements and the requirements of the Fourth Amendment."

[41] *See* Schulze, *supra* note 12, at 57 (noting "[b]usiness actors are more afraid of the potential future effects of the government regulating encryption, which might result in the widespread use of inferior technology.").

[42] For example, analysts predicted that the economic impact on US companies attributable to the Snowden leaks was in the range of $35 billion to $180 billion in lost revenue); *See* Budish, *supra* note 40, at 9.

mandated vulnerability;[43] (6) recognition that law enforcement has essentially lost the crypto wars of the 1990s (discussed below); (7) concern that backdoors are often mandated by authoritarian regimes to surveil a population in violation of their fundamental human rights;[44] (8) concern that on balance, society (both businesses and individuals) is safer when provided with the strongest encryption products;[45] (9) an argument that law enforcement can use other investigative techniques to discover high priority terrorist activity and child molestation without infringing privacy of encrypted communications.[46]

1. Law Enforcement Scope Creep from Serious Crimes into Lower-Level Crimes

When enacting a new law that undercuts privacy, an issue to consider is law enforcement scope creep or "mission creep."[47] This is a risk of enacting a law for one purpose, but then expanding its scope to other purposes. The PATRIOT Act amended a variety of statutes to broaden surveillance, including its amendment to the Bank Secrecy Act, giving the government broad access to financial information, arguably eliminating financial privacy in the United States. The primary motivation behind the PATRIOT Act was to deter terrorism, and this terrorism fear facilitated its swift enactment to increase money laundering surveillance, which is sometimes

[43] *Id.*
[44] *See* Schulze, *supra* note 12, at 57.
[45] Former NSA Director Michael Hayden belongs to this school of thought, noting that "America is simply more secure with unbreakable end-to-end encryption." *Id.* at 59.
[46] *See* Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors In The Web 2.0 Era,* 8 J. On Telecomm. & High Tech L. 360, 399 (2010) (noting "[i]f a suspect is important enough, let the police dedicate the significant manpower to break into her home in order to install bugs. Given the finite limit to the financial and human resources available to law enforcement agencies, such a change in the balance of power, by raising the effective cost of such surveillance, would force investigators to prioritize their targets, and shy away from fishing expeditions.")
[47] Fletcher N. Baldwin, Jr. & Daniel R. Koslosky, *Mission Creep in National Security Law*, 114 W. Va. L. Rev. 669 (2012), available at http://scholarship.law.ufl.edu/facultypub/243.

associated with terrorism. However, reviewing FINCEN's website reveals that the bulk of BSA violations relate to money laundering or regulatory banking enforcement actions with no identified terrorism threat (with some examples discussed below). It could be argued that the effect of the PATRIOT Act was to augment the government's money laundering investigation powers using terrorism concerns as the justification. This article does not opine on whether this reduction in financial privacy is harmful to privacy rights of law-abiding Americans, but simply observes that financial privacy rights were undercut by the PATRIOT Act's BSA amendments with terrorism concern as the motivating factor for this legislation. Whether and to what extent a free society needs strong financial privacy from government surveillance is not explored herein (e.g., arguments that a lack of financial privacy could be abused by an overreaching government or an assessment of the regulatory cost versus the amount of crime detected).

Another possible example of mission creep can be observed in that laws allowing surveillance for national security purposes can uncover evidence that may be used in ordinary criminal investigations. A concern is that if the Executive Branch has very broad surveillance powers in the national security context, then this could lead to a police state where ordinary crimes are routinely investigated under the guise of national security. However, courts have noted that although evidence obtained under FISA subsequently may be used in criminal prosecutions, "the investigation of criminal activity cannot be the primary purpose of the surveillance."[48]

A similar concern of mission creep should be contemplated with new legislation focusing on CP. Just as terrorism concerns provoke an emotional, fearful response in the population that facilitates a willingness to reduce personal privacy rights, the same can be said about CP, which often involves heart-wrenching stories of abused children. Therefore, new CP legislation should be approached cautiously, factoring any detrimental effects on privacy rights in

[48] In re Sealed Case, 310 F.3d 717, 726-27 (F.I.S.C. 2002).

society overall as well as the effectiveness in combatting CP versus and whether the effect of a new law will largely increase police powers for non-CP crime enforcement under the guise of combatting CP.

There is a general concern of government seizing too much power over a society. One author provides several salient points on this concept: "On the side of the government, there exists an independent desire to promulgate its ideas and to survive, and it will take whatever actions it deems necessary to do so."[49] "The expendability of rights is more than a government contrivance. Americans have been willing to relinquish their individual rights (1) in response to fear, or (2) when the government has been able to convince Americans that it is in their best interest to forgo their liberties in lieu of their safety."[50] "Americans are willing to forgo their rights during wartime, but there is a quiet expectation that once the threat has subsided, homeostasis returns."[132] "While there is a line of reasoning that the war on terrorism is an ongoing one, because of the very nature of this war and its duration, our government should exercise greater care in passing laws that affect constitutionally protected rights. Congress must consider that laws in response to a continuous threat have the potential to become firmly entrenched in our criminal justice system. Therefore, such laws should be focused and temporary. The Patriot Act is neither. It is not a routine response during a time of turmoil. This particular piece of legislation subverts checks and balances, ignores constitutional conflicts, and assumes a permanent place in American law."[51]

Another observation is that once legislation grants the government certain powers it can take some effort to negate overreach either by judicial ruling or subsequent legislation. In the surveillance context, the PATRIOT Act granted broad surveillance

[49] Metzler, Christopher, *Providing Material Support to Violate the Constitution: The USA Patriot Act and Its Assault on the 4th Amendment*, 29 N.C. Cent. L.J. 35, 50 (2006).
[50] *Id.* at 52.
[51] *Id.* at 52 – 53.

powers, but it was not until more than a decade later, when Congress cut back on some of that PATRIOT Act surveillance authority (e.g. some limits on bulk collection) through the USA Freedom Act, enacted in 2015 in response to the Edward Snowden leaks concerning mass government surveillance.[52]

Law enforcement and the U.S. government have tools available for terrorism or other serious crimes that might also be used for lower-level crimes. There is also evidence of law enforcement using such tools for more expansive uses unrelated to terrorism detection. The Snowden leaks concerning the lack of adequate privacy protections against government surveillance in the US exemplifies the lack of transparency that exists concerning the vast data on individuals the government has the ability to collect.[53] Federal law enforcement have routinely used Suspicious Activity Reports (SARs) to convict drug dealers, even though a major motivation of establishing SARs post PATRIOT Act was in response to terrorism concerns. In one case, federal investigators prosecuted a student at a university for shipping marijuana and selling to distributors at his university.[54] The use of the Financial Crimes Enforcement Network (FinCEN) under the Bank Secrecy Act (BSA) to help federal investigators to convict drug dealers is common occurrence.[55] Similarly, the FBI has launched an encrypted phone service called

[52] *See* Margaret Hu, *Bulk Biometric Metadata Collection*, 96 N.C. L. Rev. 1425 (2018).

[53] Anthony Volini, *A Deep Dive into Technical Encryption Concepts to Better Understand Cybersecurity & Data Privacy Legal & Policy Issues*, 28 J. INTELL. PROP. L. 291, 354 (2020).

[54] Financial Crimes Enforcement Network, *SARs Help Bust $1 million Drug Ring Led by Significantly Older Student*, The SAR Activity Review, Issue 23, Story 6 (May 2013), https://www.fincen.gov/sars-help-bust-1-million-drug-ring-led-significantly-older-student.

[55] *Id.*; Financial Crimes Enforcement Network, *Suspicious Activity Reports Aid Conviction of Drug Dealers*, The SAR Activity Review, Issue 7 (August 2004), https://www.fincen.gov/resources/law-enforcement/case-examples/suspicious-activity-reports-aid-conviction-drug-dealers; *See generally* Financial Crimes Enforcement Network, *The Value of FinCEN Data*, https://www.fincen.gov/resources/law-enforcement/case-examples?field_tags_investigation_target_id=670.

Anom that permits the FBI access to users', who are frequently drug traffickers or other organized criminals, messages much like a back door.[56] The phone service secretly accessed and obtained about 27 million messages between 2019 and 2021.[57] The value of access to these tools, data, and information is clear. The possible scope creep into lower crimes and individuals' lives is a reason to be concerned with allowing law enforcement overly broad access to private information.

An example of law enforcement scope creep could include the implementation of community policing. The original point of community policing was to increase the involvement of ordinary citizens in policing neighborhoods. However, there are many instances of law enforcement personnel commandeering community policing programs.[58] In addition to law enforcement leaders being politically motivated, the police have been "made safer" under the guise of "community policing." Community policing was supposed to help communities achieve safety without police who use a "weapons system" that makes everything, including innocent individuals, look like a criminal or serious crime.[59] Government leaders attempting to invest in community safety programs that provide safety without regular law enforcement who carry weapons to enforce the law, the police and other higher-level law enforcement individuals, like SWAT, are the exact people being hired to staff these programs.[60] In the U.S. historically, the police have been the answer for every community issue that involves disturbance or crimes. Even attempting to drift away from using law enforcement in every situation, law enforcement agencies have found ways to insert themselves into

[56] Adi Robertson, *The FBI secretly launched an encrypted messaging system for criminals*, The Verge, Vox Media, (Jun. 8, 2021), https://www.theverge.com/2021/6/8/22524307/anom-encrypted-messaging-fbi-europol-afp-sting-operation-trojan-shield-greenlight.
[57] *Id.*
[58] J. Berkeley Bentley, *Mission Creep: The Danger of Blurring Police Blue with Soldier Green (Part 3 of 3),* Huffpost (June 4, 2015), https://www.huffpost.com/entry/mission-creep-the-danger_b_7512814.
[59] *Id*.
[60] *Id.*

community issues like mental health incidents[61] when a different program may or is supposed to exist to help in those cases.

There is an ever-present concern of law enforcement overreach which supports arguments against a front door. New statutes and judicial opinions constantly evolve to counter law enforcement's natural tendency to overreach. For example, police deceiving minors has been an issue for some time and by giving them a backdoor this may increase in order for them to fulfill their objectives. Illinois passed a law that bans the use of deception by law enforcement with minors and will go into effect on January 1st, 2022.[62] This law arises amidst the evidence of law enforcement increasingly using this tactic to secure convictions. As shown by data collected by the Innocence Project, 30% of wrongful convictions were achieved by law enforcement use of deception with children and later overturned through DNA evidence.[63] These statistics and Illinois' decision to enact this law creates concern for providing a front door on the federal level for CP. With a front door, law enforcement in a state where there is no law banning deception with a minor, could potentially creep into areas of communities and individuals lives in a way they have not before. This popular law enforcement tactic could make a front door a potentially abusive tool that would lead to many innocent or non-CP related arrests and convictions.

---

[61] Andre Mouchard, *A question after George Floyd: What do we want police to do?*, Mercury News (August 23, 2020), https://www.mercurynews.com/2020/08/23/a-question-after-george-floyd-what-do-we-want-police-to-do/.

[62] Bryan Pietsch, *Illinois is first state in U.S. to ban police from lying to minors during interrogations*, The Washington Post (July 16, 2021), https://www.washingtonpost.com/nation/2021/07/16/illinois-police-lying-ban/; Innocence Staff, *Illinois Becomes the First State to Ban Police from Lying to Juveniles During Interrogations*, Innocence Project (July 15, 2021), https://innocenceproject.org/illinois-first-state-to-ban-police-lying/.

[63] *Id.*

2. Safeguards Not Being Observed by Law Enforcement and Lack of Transparency with the Public

Certainly, attorney client privilege is a safeguard for those seeking legal advice which should be respected by law enforcement; however, concerns have arisen of mass surveillance that does not safeguard privileged communications. Specifically, the New York Civil Liberties Union issued a report in 2020 discussing how attorneys can increase their use of encryption to protect client information from being sucked up by mass government surveillance particularly in criminal defense representation.[64] The report notes that "[p]rivileged and confidential attorney-client communication is illegally being recorded as a matter of course by contractors working for the government, like the telephone system contractor Securus."[65] This report supports that there is a real concern in both the EU and the US over warrantless and technologically easy government surveillance of communications and the need to protect communications from this surveillance. Interestingly, the New York Civil Liberties Union report encourages the use of open-source encryption tools that would seem to remove the possibility of a private party providing a back door to its encryption products.[66]

There is a lack of public transparency over existing tools already available to law enforcement. Law enforcement is not informing the public that law enforcement across the country is regularly able to

---

[64] *See* Jonathan Stribling-Uss, *Legal Cybersecurity in the Digital Age*, New York Civil Liberties Union at *3, https://www.nyclu.org/sites/default/files/field_documents/20200924_nyclu_legalcybersecurity_final_2.pdf. The report outlines "concrete, accessible steps that legal organizations, especially criminal defense lawyers, can do right now to ensure their attorney client communications are not sucked up into a government surveillance database or stolen by hackers."

[65] *Id.* at 14-15.

[66] *See* https://www.nyclu.org/sites/default/files/field_documents/20200924_nyclu_legalcybersecurity_final_2.pdf at page 19 ("attorneys should seek open-source products whose source code can be publicly accessed and vetted –to ensure there are no secret, government-prompted flaws that risk revealing client information.").

break into phones – even small police departments have the capability, or they simply need to send the phones to a lab.[67] Perhaps it is understandable for law enforcement not to publicly disclose the investigative tools in its arsenal and its success rate (given that this would publicly inform criminals of law enforcement's strategies and tactics). However, law enforcement's sales pitch to the public makes it sound like police are never able to break into encrypted phones, and this is not true. Jennifer Granick, a cybersecurity lawyer at the American Civil Liberties Union explains "Law enforcement at all levels has access to technology that it can use to unlock phones. That is not what we've been told."[68] The truth it would seem is that sometimes they can break in and sometimes they cannot, with one Manhattan prosecutor explaining "we may unlock it in a week, we may not unlock it for two years, or we may never unlock it."[69]

Certain branches of the government already have or are able to obtain back doors with some contracted companies. The NSA has contracted agreements with tech companies that would provide similar features that essentially equate to a back door.[70] The NSA has had to change its policies concerning seeking these agreements by weighing the costs and benefits of such an agreement being accidentally used by a bad actor.[71] These changes are in response to actual incidents of bad actors taking advantage of these contracts and back door technology.[72] These incidents will be discussed further below. The failure by the NSA to have enacted sufficient safeguards to already available government backdoors creates concerns as to all government agencies' abilities to safely use

[67] Jack Nicas, *The Police Can Probably Break Into Your Phone,* The New York Times (Oct. 21, 2020), https://www.nytimes.com/2020/10/21/technology/iphone-encryption-police.html.
[68] *Id.*
[69] *Id.*
[70] Joseph Menn, *Spy Agency ducks questions about 'back doors' in tech products*, Thomson Reuters (October 28, 2020), https://www.reuters.com/article/us-usa-security-congress-insight/spy-agency-ducks-questions-about-back-doors-in-tech-products-idUSKBN27D1CS.
[71] *Id.*
[72] *Id.*

backdoors – especially agencies who are not intimately familiar with technology or unfamiliar with backdoors in particular.

There is an inherent difficulty in policing the police. As noted earlier, law enforcement has crept its way into staffing community safety programs and that is in part an issue of government leaders failing to regulate and properly implement the programs proposed and enacted.[73] In the wake of George Floyd, some proposals of police reform have included increasing transparency of police misconduct because of the clear evidence that police use excessive force.[74] Law enforcement mission creep into mental health issues is also why increased transparency of police misconduct is recommended.[75] Allowing a front/back door for CP may give law enforcement access to sensitive citizen information and invade into unintended areas of communities. With the historical reality that police at times have overreached and are not always properly watched and regulated by government leaders, even implementing safeguards may not be enough to prevent unintended harmful consequences to society if front/back door access is available.

3. Government Front/Back Doors Have been Exploited by Bad Actors

One example that exemplifies some of the arguments against a front (or back door) for the government or law enforcement is shown by the recent SolarWinds hack. A few sources suggest that there may have been weakness on account of government backdoors that took part in allowing the success of the attack.[76] The

[73] Bentley, *supra* note 60.
[74] Mouchard, *supra* note 63.
[75] *Id.*
[76] Shawna Chen, *Dozens of Treasury email accounts breached in SolarWinds hack*, AXIOS (Dec. 22, 2020), https://www.axios.com/solarwinds-hack-treasury-email-accounts-breached-e6a24240-2795-4c09-9056-b53f20e47f37.html (noting Ron Wyden, Treasury Finance Committee Ranking Member, stated, "Finally, after years of government officials advocating for encryption backdoors, and ignoring warnings from cybersecurity experts who said that that encryption keys become irresistible targets for hackers, the USG

SolarWinds incident left almost 18,000 customers, including many high-profile clients, with updates that left them vulnerable to malicious actors.[77] In the SolarWinds attack it is believed that Russian Intelligence infiltrated the Orion system and added malicious code.[78] Perhaps the largest issue with these types of attacks is that once they occur, the harm can be long lasting and difficult to fix: "[n]ow that multiple networks have been penetrated, it's expensive and very difficult to secure systems. . . [a] former homeland security officer, said that it could be years before the networks are secure again. With access to government networks, hackers could, 'destroy or alter data, and impersonate legitimate people.'"[79] Accordingly, it seems attacks exploiting backdoors affect can have long lasting serious consequences, leaving networks and systems unsecure for years.

The SolarWinds issue shows the widespread effect of bad actors exploiting any possible doorway or entryway. Thus, having a built-in back door raises a strong possibility that it would be compromised as bad actors will earnestly attempt any possible entry into computers. The SolarWinds issue also highlights the long-term impact of exploitation of back doors by bad actors. Permitting them with more transparency and clear permission under the law is not likely to prevent this danger.

---

has now suffered a breach that seems to involve skilled hackers stealing encryption keys from USG servers,"); *See also*, Glyn Moody, *The widening Solarwinds debacle shows why the reckless idea of backdooring encryption must be dropped forever*, Privacy News Online (Dec. 24, 2020), https://www.privateinternetaccess.com/blog/the-widening-solarwinds-debacle-shows-why-the-reckless-idea-of-backdooring-encryption-must-be-dropped-forever/ (noting, "key to the intrusion was the insertion of malicious code into the Orion network monitoring software from SolarWinds – a backdoor in software that was very widely used and trusted.").

[77] Isabella Jibilian and Katie Canales, *The US is readying sanctions against Russia over the Solarwinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal*, Business Insider (April 15, 2021).

[78] *Id.*

[79] *Id.*

Secret encryption has been championed as a threat to national security by some intelligence officials.[80] The NSA has employed contracts with technology companies to procure back doors without a warrant in response. Yet, these back doors have proven just as great a threat as the championed threat to national security by intelligence officials. In 2015, the Juniper Network had an incident where they found malicious code in some firewall products that was supposedly placed by Chinese government hackers.[81] Legislators have considered the issue of these covert agreements between the NSA and tech companies, but as of yet, the NSA continues to champion the idea that tech companies working with them covertly is too valuable a national security asset.[82]

Considering incidents like the Juniper Network and SolarWinds incidents, there is clearly a great threat to national security as much as there is a valuable asset for national security. The fact that there are covert underregulated back doors being used today, is a greater threat due to the lack of transparency to citizens. Permitting a back door is more than giving law enforcement the ability to investigate more complex crimes but also about creating a crack in some of the most secure firewalls and cybersecurity tools in a world where the Internet and technology are much more complex and pose greater dangers if not buttoned up.

4. Difficulty in Designing Breakable Encryption Products that Still Provide Strong Protection

Today, the US economy is based largely on online shopping and other online transactions which leave consumers open to many security and privacy concerns. The ideals of security and freedom on the internet have shifted slightly, but the same economic and security preferences exist. As footnoted in Part 1, Congress is currently contemplating a bill called the Lawful Access to

[80] Menn, *supra* note 72.
[81] *Id.*
[82] *Id.*

Encrypted Data. This bill would require tech companies to put backdoors in their products to allow law enforcement access to customer's data with a warrant.[83] Creating security in technology is no easy task and has taken a long time but is being undermined by this push for back doors and for tech companies to comply with law enforcement requests in such proposed bills.[84] Any of the proposals that have been made over the past few decades have high administrative costs to consumers, government agencies, and businesses. The complexity of designing security products has also only increased with time. The playing field may have upgraded, but the social concerns, security product design success rates, and economic cost of implementing such backdoor law enforcement access regulations has remained relatively the same.

Generally, strong encryption is desirable in IT products, and the longer and more complex the encryption key is, the less susceptible the product is to attack.[85] However, implementing the strongest encryption possible will make no difference if a back door is provided to bypass that strong encryption. To use a simple analogy, one could fortify the front door to a house with multiple locks, but if there is a known way to easily open the back door, then fortifying the front door was wasted effort.

5. Consumers Purchases of Foreign Encryption Products Creating Anticompetitive Effects for U.S. Products

Mandating a back door in U.S. products may increase the number of U.S. and foreign consumers purchasing foreign encryption products to avoid the inherent security shortcomings of the U.S. product. Consumer data is used in online searches and

[83] Catherine Chen, *Bill That Mandates Cyber Backdoors Will Leave Front Doors Wide Open*, CPO Magazine (July 21, 2020), https://www.cpomagazine.com/cyber-security/bill-that-mandates-cyber-backdoors-will-leave-front-doors-wide-open/.
[84] *Id.*
[85] Mohit Arora, *How secure is AES against brute force attacks*, EE Times (May 5, 2012), https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/.

social media and helps drive companies' profits. [86] As consumer data increasingly becomes a commodity, data privacy law conflicts will also become an increasingly important factor in consumer decisions of products.

Laws around the globe affect the encryption products that can be created by companies in certain countries which can affect the competitiveness of these companies' products. The European data privacy protection law, the General Data Protection Regulation (GDPR) favors individual's privacy.[87] The GDPR has inspired development of stronger security and privacy law throughout the U.S. and the entire world (e.g., California's recent privacy statutes and similar laws emerging in other U.S. states). The GDPR includes Article 25 requiring security and privacy by design and default, and presumably many regions around the globe have developed and will develop similar legal requirements. Thus, the sale of an IT product having strong encryption, unbreakable by private or government actors, would be a valuable competitive product worldwide as it would be GDPR compliant and potentially compliant with new security/privacy laws in countries outside of the EU.

Whereas U.S. privacy laws generally support competition because it is more of a hodgepodge of laws focused on specific areas of privacy rather than privacy at large.[88] U.S. privacy laws, however, are trending towards a similar general privacy law setup as they continue to cover more areas and take inspiration from the GDPR.[89] The hodgepodge version of U.S. privacy laws makes producing strong encryption products in the U.S. and purchasing those products preferable. So, while consumer data increases in value as a commodity, it is at odds with the importance of an individual's data privacy.

[86] Erika M. Douglas, *The New Antitrust/Data Privacy Law Interface*, The Yale Law Journal Forum, 659 (January 18, 2021).
[87] *Id.* at 675-676; *See generally* GDPR, https://gdpr-info.eu/.
[88] *See generally* Douglas, *supra* note 88, at 659.
[89] *See generally Id.* at 657-661.

To some extent, the less restrictive privacy laws have made the U.S. market more appealing to businesses and consumers. While U.S. laws becoming more similar to the GDPR, in some respects, levels the playing field to some extent, the introduction of a front door would likely shift the competitive edge to foreign products, especially with concern to encryption and privacy products. While in some cases the use of encryption and privacy tools, such as onion routing, may be seen as suspicious and susceptible to use by bad actors, there are many individuals who appreciate and want their privacy to the most secure extent. In a world where the internet and social behavior has made sharing one's life the norm, there are many who would prefer to avoid that lifestyle for something that seems to be from an age of bygones. Many consumers want their lives to be private and secure. Many want little government interference. Thus, a front door may become a hindrance to the competitive ability of U.S. encryption and security products.

While there is a trend to a more unified privacy regulation system that favors individual privacy, there have already been rules issued that raise the concern on the competitiveness of US encryption products. Recently, an executive order was issued that increased the priority of sharing information and data to the government in situations of cybersecurity and threats.[90] This order is on par with the trend of orders that have promoted government access to more information and consumer data for security purposes.[91] This trend shows that the front door may be available on the horizon, however, with the competitive interest at risk, the

[90] *Executive Order on Improving the Nation's Cybersecurity*, The White House Briefing Room (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; *See generally* Scott A. Schipma and Paul F. McQuade, *Executive Order on Improving the Nation's Cybersecurity: An Ambitious and Timely Call for a Broad Range of Cybersecurity Improvements,* Greenberg Traurig (May 24, 2021), https://www.gtlaw.com/en/insights/2021/5/executive-order-improving-us-cybersecurity-ambitious-timely-call-cybersecurity.

[91] U.S. Department of Commerce, *International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally* (June 26, 2017), https://www.commerce.gov/files/international-cybersecurity-priorities-fostering-cybersecurity-innovation-globally-june-26.

U.S. government may likely stick to its historical stance on the data privacy versus competition divide: voting against a front door.

6. Law Enforcement Essentially Lost the Crypto War of the 1990s

For decades, policy makers pushed for the twofold goal of (1) making the Internet safer and build impenetrable cybersecurity while (2) allowing the government access to data. In the 1990s, the push was for the Clipper Chip, a proposal which stressed the importance of strong security while trying to permit government agents to obtain keys to decrypt when needed through legal means.[92] The key would have been imposed domestically because US companies are likely to only sell domestically to reduce costs.[93] There was concern about the security of creating such a key in a society that favored privacy and freedom over government interference to provide national security.[94] Economically, imposing such a regulation would have posed a great burden on companies' administration and this regulation did not fit the ideals of US society at the time. There was no realistic proposal to ensure the strictest security in permitting the government agencies to obtain a key either.

Bernstein v. U.S. Department of State[95] provides a helpful discussion of the history of the government's attempt to regulate encryption, initially through the Arms Export Control Act and its accompanying regulations, and then through the Export Administration Act of 1979 and its accompanying regulations.[96] In *Bernstein*, a mathematician sought a declaratory judgment that his

[92] William A. Hodkowski, *The Future of Internet Security: How New Technologies Will Shape the Internet and Affect the Law*, 13 SANTA CLARA HIGH TECH L.J. 217 (1997).
[93] *Id.* at 246-247.
[94] *Id.* at 236-237.
[95] 974 F. Supp. 1288 (N.D. Cal. 1997).
[96] As explained in *Bernstein*, On December 9, 1996, President Clinton, via Executive Order 13026, transferred jurisdiction over the export of nonmilitary encryption products to the Department of Commerce under the Export Administration Act of 1979, 50 U.S.C. §§ 2401–2411 (1991) and the Export Administration Regulations, 15 C.F.R. §§ 730.1–.10 (1997). Bernstein, 974 F. Supp. at 1291.

publication of encryption algorithms was First Amendment protected, thereby negating enforcement under the regulations of the Arms Export Control Act and the regulations of the Export Administration Act.[97] The court sided with the Plaintiff, holding that the encryption regulations were unconstitutional prior restraints in violation of the First Amendment.[98] The decision in *Bernstein* and related cases, along with other public debate, likely paved the way for the U.S. Government in 1999 to ultimately forego regulation of commercial encryption products.[99]

If law enforcement continues to lose the crypto wars with privacy interests outweighing crime detection, then perhaps a fundamental privacy principle is taking shape equivalent to the English and US criminal concept of Blackstone's ratio: "it is better that ten guilty persons escape than that one innocent suffer." Blacktsone's ratio is credited with the development of the beyond reasonable doubt standard in criminal law and likely influenced development of other constitutional protections within the US.[100] Roughly applying this same principle to privacy, one could argue that it is preferable to allow a certain amount of unsurveillable criminal communications rather than undermine the privacy interests of millions of law-abiding civilians. If the US supports unsurveillable communications, this could potentially overrule law enforcement's long-standing request to have a readily available encryption backdoor, which companies such as Apple have resisted.[101] While this extremely pro-privacy view is appealing, it could pose some dangers as noted below. That being said,

[97] Bernstein, 974 F. Supp. at 1291.
[98] *Id.* at 1308.
[99] *See* Swire & Ahmad, *supra* note 7 (noting at page 416 that "[i]n 1999, . . . the administration shifted position to allow largely unrestricted export of encryption technologies. Encryption law and policy discussions largely faded from view.").
[100] For some general discussion and critique of Blackstone's ratio, *see* Daniel Epps, *One Last Word on the Blackstone Principle*, 102 VA. L. Rev. Online 34 (2016).
[101] Lauren Feiner, *GOP senators introduce bill that tech advocates warned would weaken privacy*, CNBC (June 24, 2020, 9:47 AM), https://www.cnbc.com/2020/06/24/gop-senators-introduce-bill-that-would-create-a-backdoor-for-encryption.html.

concerning EU-US data transfers, if a strong terrorism concern exists regarding such a transfer, law enforcement could potentially order a tech provider, through the courts, to hand over the key, assuming the tech provider maintains a key/the ability to decrypt.

7. Backdoor Mandates by Authoritarian Regimes Violating Fundamental Human Rights

As noted earlier, a front door regulation enacted based on CP concern could end up being abused to investigate ordinary crimes in a manner that would bypass constitutional protections. The possibility of overreach should not be ignored.

The potential for fearmongering by policy makers should not be ignored. Preying on fears held by the general public can certainly be an effective method to enact a new law, such as fear of terrorist attacks, harm to children, or exponential increase in crimes. Such fears can end up supporting enactment of laws, which might provide the government with excessive power that could be abused.

The U.S. has a history of racist fearmongering campaigns in criminal settings. The U.S. has been on the path to reforming the cash bail system, but some law enforcement, legislators, and communities have used fear mongering tactics to push their racially biased motives.[102] Opponents to the reform of the cash bail system have made arguments that bail reform is a public safety issue, is anti-police, and mischaracterize arrested individuals, especially minorities, as seriously dangerous people who need to be kept in jail even before a conviction.[103] Legislators have also pushed laws and regulations that contradict bail reform that have no basis on facts that contradict their reasoning.[104] The cash bail system has been a

[102] Vincent M. Sutherland, *The Racist Fearmongering Campaigns Against Bail Reform, Explained*, The Appeal (June 7, 2021), https://theappeal.org/the-lab/explainers/the-racist-fearmongering-campaigns-against-bail-reform-explained/.
[103] *Id.*
[104] *Id.*

tool that has been used by racially biased and corrupt individuals to justify disproportionate and unfair arrests of vulnerable people.

The history of the U.S. using seemingly justified motives to ensure public safety is why the motives of a law enforcement pushing for a front door should be cause for concern. While CP is a real issue, there is certainly some concern of law enforcement favoring a front door for other motivations or using a front door in the future for unfair purposes. While cited motives for expansion of law enforcement powers include issues of terrorism and nationwide attacks, some would argue that such powers are disproportionately aimed at minorities and vulnerable populations including the Black, Latinx, Hispanic, Indigenous, Asian, Muslim, Sikh, and other frequently targeted communities. Thus, allowing a front door whether for CP or some other motive, the U.S. should be prepared for the real possibility of unjustified targeting and overreach with the justification of improving public safety.

Cybersecurity experts have also highlighted that the recently introduced Apple software tool for iPhones is at risk of being abused to violate human rights. Apple recently introduced a software tool for iPhones that flags cases of child sex abuse by scanning images that are backed up to the iCloud.[105] Experts have noted that this system is highly invasive and infringes on people's privacy and may possibly be setting a precedent for surveillance-heavy countries like China to pass laws requiring similar technology that the government could use for pushing their authoritarian regime.[106] U.S. courts have tackled similar privacy infringement in cases concerning police searching digital information from phones seized from an arrested individual without a search warrant.[107] In the Supreme court's

[105] Brian X. Chen, *The Lesson to Learn from Apple's tool to Flag Child Abuse*, The New York Times (August 11, 2021), https://www-nytimes-com.cdn.ampproject.org/c/s/www.nytimes.com/2021/08/11/technology/personaltech/iphone-update-sex-abuse.amp.html.
[106] *Id.*
[107] Riley v. California, 573 U.S. 373, 386 (2014) (holding that there is no exception under the search incident to arrest doctrine or other Fourth

reasoning in *Riley v. California*, the Court aptly noted that phones and data cloud information are a proxy for one's life.[108] The Court's explanation fits the issue experts have highlighted about Apple's software tool. The iCloud holds much more than documents and photos, which together can already describe much of a person's life.

For an authoritarian government or law enforcement acting with biased intentions, this access would provide the ability to invade a person's life on a deep level because people's lives are essentially all on technology. This invasion and potential for abuse is why a front door may lead to violations of human rights. Considering CP and how many of today's younger generation lives and breathes on social media. To be able to control and access people's data without the proper protections in place, there are many who could take advantage of this access.

Law enforcement and mass media have also perpetuated conspiracy theories and fears arguably for their own purposes. One such conspiracy issue is the Satanic Panic. The societal fear of satanic cults began in the 1980s and persists today; the Satanic Panic is an abusive fear mongering mechanism that is "the same as those of previous periods of mass hysteria, from witch hunts to McCarthyism.[109] This fear mongering is why some individuals are still in jail after persecution without evidence by biased law enforcement feeding off the social concern.[110] Recently, Satanic Panic has been used to accuse Lil Nas X of being a corrupting influence.[111] Law enforcement and legal entities have thoroughly proven that this panic is an irrational fear that has only resulted in other injustices such as the spread of misinformation of AIDS and persecution of the LGBTQ community for false claims of satanic

Amendment doctrine exception that would allow police to search digital information from a phone seized from an arrested individual.).

[108] *Id.* at 394-397.

[109] Aja Romano, *Why Satanic Panic never really ended*, Vox (March 31,2021, 2:50 PM), https://www.vox.com/culture/22358153/satanic-panic-ritual-abuse-history-conspiracy-theories-explained.

[110] *Id.*

[111] *Id.*

involvement.[112] The long and persistent Satanic Panic is an example of using spiraling investigations and wild claims of dangers to national security that are a serious potential threat into people's privacy and personal information. With a "phone acting as a proxy for one's life" law enforcement could use front door access while continuing to present no evidence to invade privacy on the claim that they will find evidence.

a. Apple's Perceptual Hashing Technique

A form of back door, designed by Apple to detect possible CP, is called "neuralMatch." The tool will scan images before they are uploaded and any matched images will be reviewed by a human.[113] Notably, this scan will be a local scan of the device rather than the Cloud. If the matched image is confirmed as CP, the user's account will be disabled, and Apple will notify the National Center for Missing and Exploited Children.[114] Using this alternative technique may be a useful and effective way of combating CP early on as the detection process occurs before they are uploaded to the Cloud.

Perceptual hashing has an advantage over cryptographic hashing in that perceptual hashing will look for similarities between two images, while a cryptographic hash is used to detect whether a suspect image is identical to a known image. In this regard, a bad actor could make small changes to a known illegal image (e.g., add a couple of pixels) and would bypass detection of a cryptographic hash; however, the perceptual hashing algorithm should still detect substantial similarity between the two images.

The inner mechanisms of the neuralMatch scan and perceptual hashing techniques work by using an algorithm that uses a 96-bit

[112] *Id.*
[113] Frank Bakjak and Barbara Ortutay, *Apple to scan U.S. iPhones for images of child sexual abuse*, The Associated Press (August 6, 2021), https://apnews.com/article/technology-business-child-abuse-apple-inc-7fe2a09427d663cda8addfeeffc40196.
[114] *Id.*

unique identifier to match images that are the same or very similar.[115] It is possible for two images to have the same dataset but to be different images resulting in a false positive match, however, Apple claims their system only found 3 false-positives in a test of 100 million.[116] According to Apple, such false positives and any other matches will be verified and reviewed by an independent network before escalating the situation to law enforcement.[117]

Perceptual hashing has been successfully used in various contexts.[118] For example, perceptual hashing has been used to check for copyright infringement of images or works.[119] A common site that uses perceptual hash is YouTube which will screen videos when uploaded and review videos that have been flagged by users or copyright holders.[120] Considering copyright infringement, there have often been false positives that sometimes leave users at a disadvantage and inability to upload new works.[121] These applications highlight the success and issues of perceptual hashing and how individuals encounter it in their everyday lives.

Perceptual hashing shows some potential to combat CP given its success in other areas. However, care should be exercised with

---

[115] Brad Dwyer, *ImageNet contains naturally occurring NeuralHash collisions*, Roboflow, Inc. (August 19, 2021), https://blog.roboflow.com/neuralhash-collision/.
[116] *Id.*
[117] *Id.*
[118] Pete Wayner, *What is a perceptual hash function?*, VentureBeat, (August 24, 2021, 4:40 PM), https://venturebeat.com/2021/08/24/what-is-a-perceptual-hash-function/; *See also* Evan Klinger and David Strakweather, *pHash*, The Open Source Perceptual Hash Library, https://www.phash.org/.
[119] Pete Wayner, *What is a perceptual hash function?*, VentureBeat, (August 24, 2021, 4:40 PM), https://venturebeat.com/2021/08/24/what-is-a-perceptual-hash-function/; *See also* Evan Klinger and David Strakweather, *pHash*, The Open Source Perceptual Hash Library, https://www.phash.org/.
[120] Kate Klonick, *The New Governors The People, Rules, and Process Governing Online Speech*, 131 Harv. L. Rev. 1599 (2018); *See also* Rfraimow, *Adventures in Perceptual Hashing*, American Archive of Public Broadcasting, (April 20, 2017), https://blog.americanarchive.org/2017/04/20/adventures-in-perceptual-hashing/.
[121] *Id.*

respect to issues of false positives or even the possibility of bad actors injecting poisoned images onto an innocent users device. As mentioned in the previous section, care should also be taken to minimize putting society at risk of violation of human rights if for example perceptual hashing is used for mass surveillance and detection/prosecution of ordinary crimes unrelated to CP. The viability of a tool such as Apple's neuralMatch will have to be followed closely in the future. As some advocates and researchers have stated, this hashing tool essentially gives law enforcement, governments, and anyone with access to scanning and searching personal devices for any possible illegitimate act which is dangerous on multiple facets: for businesses, national security, public safety, and privacy.[122]

8. Society is Safer When Provided with the Strongest Encryption Products?

If privacy interests favor warrant proof encryption technologies, this raises a fundamental question of the value of privacy in a free society balanced against the need or desire for law enforcement to investigate criminal or terrorist activity. Likewise, this raises a larger related question, beyond the scope of this article, of what it means to live in a free society and how privacy rights fit within that free society. Certainly, if the government or private organizations (or some combination of the two) can easily review everyone's communications from both a routing standpoint (i.e., the "from" and "to" fields of a data packet) and a content standpoint (i.e., the payload of a data packet), then this unfettered access to emails, text messages, voicemails, search history, and current/past location may exemplify a society that is not free. Strong encryption can thus be a helpful tool to increase freedom through privacy of communications, hiding not only the routing info/identity of the communicating parties (e.g., "from" and "to" info) but also the contents of the messages themselves (e.g., payload of data packets).

[122] Kellen Browning, *Cybersecurity Experts Sound Alarm on Apple and E.U. Phone Scanning Plans*, New York Times, (Oct. 14, 2021), https://www.nytimes.com/2021/10/14/business/apple-child-sex-abuse-cybersecurity.html.

US government policy, both legislative and judicial, may thus continue to shift toward stronger protection of personal data.[123]

Although there are theories that data privacy and use of data as a competitive tool are integrated and interconnected components, there is a "separatist" theory that data privacy and competitive tools should remain separate. This separatist thought is focused on the idea that society is safe and has an inherent need for secure privacy and the competitive aspect of data should be considered separately.[124] The FTC has faced situations in which their competing duties concerning competition and privacy clashed, and typically the winning factor in their decisions is competition even though privacy could be just as convincing.[125] This de facto consideration is concerning as it shows people's lives, that technology and a phone act as a proxy for and hold all of the information via data, is no longer being considered a "life" but rather another commodity. Privacy should be considered a greater and more important factor than competition. The GDPR and other privacy programs tend to lean that way, but the U.S. is seemingly trending away from accepting that data today is essentially like one's diary and photo books in the past. Arguably, strong encryption products are the principal way to ensure that people's lives which today exist in essentially identical digital format and in physical tangible day to day activities are protected and not seen as a commodity.

9. Law Enforcement Can Use Other Investigative Techniques Without Infringing Privacy of Encrypted Communications

Decrypted access to individuals' data would make law enforcement's work simpler, but this access may not be necessary

[123] Riley v. California, 134 S. Ct. 2473, 2490 (2014) noting that "many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives-from the mundane to the intimate." In my view, this evidences the judicial awareness of highly personal data maintained by many people in the United States and the need to safeguard this same data.

[124] Douglas, *supra* note 88, at 653-656.

[125] *Id.*

to their work. There are arguments that law enforcement could acquire court orders to compel an individual to give law enforcement access to their password protected devices.[126] Law enforcement often cannot compel individuals to enter passwords because this raises Fifth Amendment issues.[127] So, unless there is an amendment to the law, court orders or search warrants may be alternative techniques that law enforcement may use and are already familiar with.

Courts have held that police may search data on devices, such as a phone or computer, if they first secure a warrant before conducting such a search but the search incident to arrest does not permit police officers to search data on technology present at the time of the arrest.[128] This restriction is no greater than the jurisdictional requirements set by the Pen Register Trap and Trace Statute[129] or the Wire Tap Act[130] which are used for similar purposes as what a Front Door may be used for.[131] Thus, police have used court orders and search warrants to obtain data and other information that can only be obtained through searching technology in some manner.

Using a search warrant and other means to obtain an extensive, and possibly overbroad, amount of data information is not foreign to police. Investigators can serve keyword warrants which ask

---

[126] Reema Shah, *Law Enforcement and Data Privacy: A Forward-Looking Approach*, Yale L.J. p. 555 (2015).
[127] *Id.*
[128] Riley v. California, 573 U.S. at 386 (Reasoning that there are no comparable risks of destruction of evidence as found in other search incident to arrest cases when the search is of digital data); *See also* Shah, *supra* at 128, at 547-549.
[129] The Pen Register Trap and Trace Statute requires law enforcement to get a court order.
[130] The Wire Tap Act has a "warrant plus" requirement which is a higher standard than obtaining a regular warrant.
[131] 18 U.S.C. 2701; 18 U.S.C. 3121; *see also* Center for Democracy and Technology, *CDT's Analysis of S. 2092: Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections* (2000), https://cdt.org/wp-content/uploads/security/000404amending.shtml.

companies to provide information on any users who searched for the applicable "keyword" such as a victim's name or address.[132] Law enforcement have also used reverse search warrants which aid them in searching for a suspect without having an actual suspect and allow them to ask for a broad set of information to come up with an actual suspect.[133] There are apps that have sold data on users to government agencies, which could include law enforcement because it is legal for them to purchase this information.[134] Especially in situations concerning police targeting based on race or vulnerable populations, law enforcement's access to commercial and state surveillance has grown.[135] Considering the access police have and the extent to which they already use this access, law enforcement likely does not need a more easily accessible tool to search and access data.

Law enforcement does not necessarily need another avenue when they have other investigative techniques available to them. Search warrants and court orders have been available since before technology and data became important factors in individuals' lives. Law enforcement has also used search warrants and court orders to access data and information on technology for decades. Law enforcement can also use tools that are legal but not provided through the courts such as purchasing data from data brokers. There are more than enough avenues for police and investigators to obtain and access the data they need. Access to a front door might only create a new simpler avenue with fewer checks on law enforcement to obtain private data.

---

[132] Sidney Fussell, *How Your Digital Trails Wind Up in the Police's Hands*, WIRED, (December 28, 2020), https://www.wired.com/story/your-digital-trails-polices-hands/.
[133] Sara Morrison, *Read the privacy policy: police can easily get your data from third parties*, Vox Media, L.L.C., (July 31, 2021, 9:00 AM), https://www.vox.com/recode/22565926/police-law-enforcement-data-warrant.
[134] Fussell, *How Your Digital Trails Wind Up in the Police's Hands, supra* note 134; Morrison, *Read the privacy policy: police can easily get your data from third parties*, *supra* note 135.
[135] Fussell, *supra* note 134.

II. Considering Incentives to Report CP

Given law enforcement's claim that horrific CP is widespread and that they are only able to investigate the tip of the iceberg,[136] it would seem that some measures should be taken to corroborate this claim and to combat the problem. Also, given that law enforcement will likely continue to lose on its push for an encryption back door, the question remains of how society can combat secret sharing of child pornography online. In a sense, secret sharing of such contraband can never be fully eradicated as criminals (particularly tech savvy criminals) will always look for ways to hide their activities from authorities regardless of what investigative tools exist. Therefore, a sensible goal is to make such sharing difficult rather than widespread and easy. We propose exploration of a bounty or whistleblower system that might reward a recipient of child pornography for simply handing information over to authorities. To avoid a Cobra Effect (described below), a reward system should only pay a reward where the information leads to the arrest and conviction of a suspect.

The existing deterrent under U.S. law is significant jail time for possession or distribution of child pornography. A further deterrent would involve a bounty paid to anonymous or identified recipients to report child pornography to the relevant tech platform orlaw enforcement.

Under federal law, when a private individual accidentally receives child pornography, he is required to either immediately delete the content or immediately report same to authorities to avoid a criminal charge for possession of the material (however, under various state laws, IT professionals may have an affirmative duty to

[136] Michael J. Henzey, Going on the Offensive: A Comprehensive Overview of Internet Child Pornography Distribution and Aggressive Legal Action, 11 APPALACHIAN J.L. 1 (2011)(noting a 2011 DOJ report estimating the existence of 14 million child pornography websites).

report CP rather than delete).[137] In addition to avoiding a criminal charge, payment of a bounty could be a further reporting incentive for any private individual, and reporting the news of such bounty payments could stimulate further reporting.

A. Other Federal Bounty Hunter Systems and Their Effectiveness

The United States and the many federal agencies within it have long used bounty schemes to incentivize and pay informants to help infiltrate criminal organizations and to help increase the effectiveness of catching criminals and solving crimes within the United States borders.[138] The general structure of a federal bounty scheme is the federal government providing incentives to informants by offering the informants a monetary reward, such as a percentage of the legal action the government decides to take based on the information obtained by the informant.[139] The federal government essentially partners and establishes working relationships with United States citizens to help protect the people within the United States' borders by minimizing crime through voluntarily enlisting citizen informants.

The debate over whether federal bounty programs should be continued or not is generally centered on if the potential moral or ethical lines that bounty programs potentially cross is outweighed by the successful results these programs produce. However, despite

---

[137] 18 U.S.C. § 2252A(d): "It shall be an affirmative defense to a charge of violating subsection (a)(5) that the defendant--
(1) possessed less than three images of child pornography; and
(2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any image or copy thereof--
(A) took reasonable steps to destroy each such image; or
(B) reported the matter to a law enforcement agency and afforded that agency access to each such image."
Regarding state law, Illinois is one example of a state requiring an IT professional to report CP to the Cyber Tip Line at the National Center for Missing & Exploited Children. See 325 Ill. Comp. Stat. 5/4.5.

[138] Marsha J. Ferziger & Daniel G. Currell, *Snitching For Dollars: The Economics and Public Policy of Federal Civil Bounty Programs,* 4 UNIVERSITY OF ILLINOIS L. REV. 1141, 1142 (1999).

[139] *Id.*

the potential moral implications of federal bounty programs, federal bounty programs remain prevalent because they have produced successful results.[140]

Another example showing the expansion of bounty programs is the Narcotics Reward Program ("NRP") which was "established by Congress in 1986 as a tool to assist the U.S. Government in identifying and bringing to justice major violators of U.S. narcotics laws responsible for bringing hundreds of tons of illicit drugs into the United States each year."[141] The NRP, in just the past five years alone, has "distributed almost $32 million to 33 people, with some receiving as much as $5 million, according to the State Department Bureau of International Narcotics and Law Enforcement Affairs.[142] Further, since the NRP's creation, the program has resulted in the arrest of almost 70 foreign major violators.[143] Therefore, the success or effectiveness of the federal bounty programs should not be measured by the potential moral or ethical lines the programs may cross, but whether the programs are achieving the goals they were created for.

By simply looking at the results of one bounty program created by the federal government, specifically the NRP, it can be seen these programs are doing just what they intended to do. A similar program could be used with the same level of success and effectiveness if applied to CP. Such a program would provide an opportunity to citizens to help aid in the fight against CP and other child abuse crimes. Considering the sensitivity surrounding CP, a direct personal benefit may be the push citizens need to overcome the qualms against reporting incidents of CP. The partnership a federal bounty program would ultimately create between the federal government and the citizen informants is arguably essential to

---

[140] *Id.* at 1143.
[141] U.S. Dep't of State, *Narcotics Reward Program,* U.S. DEPT' OF STATE, https://www.state.gov/inl-rewards-program/narcotics-rewards-program/.
[142] Olivia Carville, *America's Multimillion-Dollar Bounty Program Just For Drug Lords,* FEDERAL PRACTICE GROUP (Nov. 9, 2018, 1:48 PM), https://fedpractice.com/2018/11/09/americas-multimillion-dollar-bounty-program-just-for-drug-lords/.
[143] *Id.*

successfully solving CP and tackling it from the beginning and its point of distribution.

The NRP is not the only example emphasizing the effectiveness of federal bounty programs. With the internet and technology continuously expanding, the federal government has also begun to develop "bug-bounty programs," as a result of seeing the success corporations have had with these types of bounty programs.[144] Bug bounty programs use computer-security experts to hack into existing infrastructures and expose existing vulnerabilities with the goal of implementing stronger security measures on the internet.[145] Examples of these bug bounty programs' recent success can be seen through Google paying out more than $2.9 million in bounties in 2017, and Apple offering up to $200,000 for the identification of certain vulnerabilities.[146] The success of these large corporation's bug bounty programs led to the creation of the SECURE Technology Act which compels the Department of Homeland Security to establish a bug-bounty pilot program.[147]

The expansion of bounty programs to the online realm further exemplifies the strength and success of these bounty programs. Not only is the federal government using these programs to solve crimes committed on the physical streets of the United States, but now the federal government is expanding these programs to the internet due to the results seen from the various other bounty programs to help prevent hackers from infiltrating governmental systems and large corporations online. Federal bounty programs may potentially cross ethical boundaries, however it is arguable these programs are absolutely essential for the most effective way of catching criminals

---

[144] Myles Ashong, *Bug the Bounty Hunter: Recommendations to Congress to Best Effectuate the Purpose of the SECURE TECHNOLOGY Act,* AMERICAN BAR ASSOCIATION (Jan. 31, 2020), https://www.americanbar.org/groups/public_contract_law/publications/public_contract_law_jrnl/49-1/secure-tech/.

[145] *Id.*

[146] *Id.*

[147] *False Claims Act,* The National Whistleblower Center, https://www.whistleblowers.org/protect-the-false-claims-act/.

on the internet and historically elusive criminals involved in crimes such as CP and human trafficking.

Other examples of bounty programs include the program in relation to the False Claims Act which provides rewards for informants who report frauds committed upon the government.[148] Sources state that the False Claims Act is one of the strongest whistleblower laws in the United States.[149] If the whistleblower's information results in a successful prosecution, whistleblowers receive a mandatory reward of 15% to 30% of the collected proceeds.[150] Similar bounty programs that share the same goals and success as the False Claims Act whistleblower program include: the SEC Whistleblower program, the CFTC Whistleblower Reward Program, and the Anti-Money Laundering Whistleblower reward program.[151]

The SEC Whistleblower program actually just issued their largest bounty award to date in 2020 with the reward totaling $114 million dollars to a whistleblower whose information led to a successful prosecution.[152] Further, "the SEC has awarded approximately $676 million to 108 individuals since issuing its first award in 2012."[153] The publication and press on the large rewards awarded, such as the SEC award to a whistleblower in 2020, will only increase individual's motivation to participate and will ultimately only enhance the success of the bounty programs.

After reviewing the results of the bounty program examples provided above, bounty programs appear to be effective. Citizens likely know their communities better and on a more personal level than the government, therefore the citizens may catch things that the

[148] *Id.*
[149] *Id.*
[150] *Id.*
[151] Jason Zuckerman & Matthew Stock, *What is a Whistleblower Reward?,* Zuckerman Law (Jan. 14, 2021), https://www.zuckermanlaw.com/sp_faq/what-is-a-whistleblower-reward/.
[152] *SEC Issues Record $114 Million Whistleblower Award,* U.S. Securities & Exchange Commission (Oct. 22, 2020), https://www.sec.gov/news/press-release/2020-266.
[153] *Id.*

government is unable to. The citizens' ability to know their communities better and the fact that they are more likely to be aware of situations of CP means that enlisting citizens to voluntarily inform law enforcement would likely increase law enforcement effectiveness in tackling CP significantly. The number of rewards issued to citizens and the number of tips provided are a testament to the effectiveness of a federal bounty hunter system. Notably, the rewards are only issued for successful prosecutions. Therefore, the numerous rewards issued yearly under the discussed programs may show insight into what is possible with the use of a CP bounty hunter system. The U.S. would not be considering the expansion of such systems into other areas of crimes if they were not successful and effective. Thus, adding CP into the continuous expansion of these bounty programs would seem to be an appropriate next step in the expansion path and in tackling CP.

B. Proposed Systems to Deter CP

Reporting and deterring child pornography can be potentially improved in different ways. They include (1) prioritizing preteen CP because they are the most vulnerable population and as children gain greater autonomy it is difficult to assess between free will and forced acts; (2) funding and use of a federal bounty hunter or tipster program as discussed earlier; (3) licensing of private researchers to corroborate law enforcement claims; (4) a private bounty hunter system; and (5) the U.S. Supreme Court could consider allowing courts to compel production of a defendant’s password or decryption key as a deterrent to CP.

1. Prioritize Preteen CP

In terms of priorities, we propose that for any improved deterrence or reporting system (whether government run or privately operated) young victims should be the highest priority, such as CP involving victims 12 and under (i.e., preteens). This is

consistent with Henzey's view that so-called juvenile self-produced child porn should be classified as a low-level misdemeanor.[154]

Prioritizing a younger group will help a clearly extremely vulnerable age group. Children of this age group are more likely to be abused and exploited.[155] Children are four times more likely to be trafficked by family members than adults are to be trafficked.[156] The main reason for child human trafficking, especially for girls, is forced sexual exploitation.[157] The larger issue with this form of human trafficking is that it is often conducted at home where children are more likely to be coerced and psychologically abused to accept the sexual exploitation.[158] Per one study, almost thirty percent of girls who are trafficked are under the age of 11 and approximately another twenty percent of girls being between the ages of 12 and 14.[159] For boys who are trafficked, approximately fifty percent of them are under the age of 11 and approximately another twenty percent are between the age of 12 and 14.[160] Looking at these numbers, while boys are less likely to be trafficked for sexual exploitation, a large portion of these children are subjected to child pornography, whether that be by being filmed and photographed while sexually exploited or exploited for the main purpose of child pornography.[161] The CP materials that come out of

[154] Michael J. Henzey, Going on the Offensive: A Comprehensive Overview of Internet Child Pornography Distribution and Aggressive Legal Action, 11 APPLACHIAN J.L. 1, 2 (2011).
[155] National Center for Victims of Crime, *Child Sexual Abuse Statistics*, https://victimsofcrime.org/child-sexual-abuse-statistics/.
[156] Counter Trafficking Data Collaborative (CTDC), *Age of Victims: Children and Adults*, "Recruiter Relationship Adults and Children", (2021) https://www.ctdatacollaborative.org/story/age-victims-children-and-adults.
[157] CTDC, *Exploitation of Victims: Trends*, (2021), https://www.ctdatacollaborative.org/story/exploitation-victims-trends.
[158] The Children's Assessment Center, *Child Sexual Abuse Facts and Resources*, https://cachouston.org/prevention/child-sexual-abuse-facts/.
[159] CTDC, *Age of Victims: Children and Adults*, "Age of Identified Girls and Boys", *supra* note 158.
[160] *Id.*; *See also* The Children's Assessment Center, *supra* note 160.
[161] CTDC, *Exploitation of Victims: Trends*, *supra* note 159; *See generally* The Children's Assessment Center, *Child Sexual Abuse Facts and Resources*, *supra* note 160; *See also* Luzwick, *supra* note 27, at 366.

human trafficking are the egregious photographs and videos that need to be targeted to end the distribution of CP and tackle CP on a wholistic level.

Preteens ostensibly have less cognitive ability to consent to any sexual interactions and the less awareness of what is happening to them compared to teens.[162] Although teens can certainly be victims, selecting a low age cutoff would likely filter out what would be classified as a low-level misdemeanor if the photos and videos were self-produced by sexually active teenagers. Many older children are still exploited for child pornography and sexual exploitation, but the mix of independent judgement and the activities of older children online makes separating exploitation and the regular activity of teens harder to distinguish.[163] Thus, in order to protect children unable to make these independent judgements and tackle an area of child pornography effectively and successfully, the suggestion in this article is to prioritize children age 12 and younger (e.g., highest awards paid for convictions relating to preteen victims). Accordingly, CP involving preteen victims could be the highest priority for detection and deterrence.

Another issue to consider is the prioritization of what type of child pornography content to search and report both from a law enforcement and private bounty hunter standpoint. For example, Henzey suggests that self-produced teen images (e.g., shared between high school classmates) should not be pursued when more egregious content may be hunted (e.g., sexual abuse of toddlers).[164] It would certainly seem strange, and invasive, to have private bounty hunters sifting through the social media content of high schoolers. Thus, a bounty program could have the greatest societal benefit and effectiveness in combating CP if it were to focus on the distribution of suspected CP images rather than self-produced

[162] CTDC, *Exploitation of Victims: Trends*, *supra* note 159.
[163] Ling-Hsiang Wang, *Credibility Judgment Predictors for Child Sexual Abuse Reports in Forensic Psychiatric Evaluations,* National Library of Medicine, Vol. 16(2) (February 16, 2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6393749/.
[164] Henzey, *supra* note 156, at 28-29.

content shared between sexually active teens, albeit these self-produced shared photos might be found elsewhere due to revenge or some other motive but that is an issue to tackle at another time.

A technology platform and organization called Thorn, founded by Ashton Kutcher and Demi Moore, aims to help law enforcement reduce trafficking of minors. Thorn's research discusses the most vulnerable victims are those under the age of 12.[165] After speaking to survivors of sexual exploitation, the organization found that the average age of victims entering sex trafficking was 14-15, and at that age group the involvement of a minor speaking to the buyer substantially increases (with the trafficker typically handling communications with sex buyers for preteen victims).[166] In one of their survivor interviews, an individual noted being born into the system and that escaping was almost an impossible task.[167] A significant number of teen victims are found to have been exploited prior to their teen years, in essentially a grooming process for victims extending through their teen years.[168] This raises the possibility of traffickers distributing CP images of preteen victims as an advertising tool to attract buyers. Thus, any reporting incentives of preteen images might have some impact in terms of reducing sex trafficking of minors and perhaps make it more difficult for a trafficker to groom and advertise preteen victims to potential buyers given a higher risk of getting caught based on rewarding the public for reporting. In theory, an anonymous reward system with substantially high rewards could potentially encourage a purchaser of a preteen victim to report the trafficker (and certainly such a system could contemplate whether and to what extent such an anonymous tipster might be shielded from liability if anonymity were compromised).

The ICMEC have also made their own missing child alert system. The system shares case information, child information accessible to the public, generates leads for investigators using

[165] Thorn, https://www.thorn.org/survivor-insights/.
[166] *Id.*
[167] *Id.*
[168] *Id.*

facial recognition to match missing child photos to data found on both the clear and dark web, and more.[169] This raises the possibility that if some form of tipster reward (either transparent or anonymous reward) might increase reporting across the board for both teen and preteen minor victims.

Certainly, further research exploring any relationship between CP and sex trafficking of minors would provide helpful insight.

2. Funding of a Federal Bounty Hunter System or Tipster Reward Program

Funding for a reward system could come from tech platforms that provide warrant-proof encryption and meet a minimum annual revenue. Funding from such platforms may be fair if they are providing platforms that facilitate secret sharing of CP (although the ostensible purpose is to promote privacy). Such platforms may contribute via charitable donations and/or a CP tax or perhaps a tax credit. A modest CP tax could be imposed on large tech platforms that provide warrant-proof encryption and have substantial annual revenue. Alternatively, users could potentially pay the tax (through their ISP). The tax revenue could be used to fund tipster programs and/or hiring of additional law enforcement investigators in the area of online CP, especially given law enforcement's claim that it is only prosecuting the tip of the iceberg. In addition, such funding might also be used for victim support, such as counseling, education, etc.

A conventional tipster reward program seems feasible, where a financial reward can be awarded for reporting information leading to arrest and conviction of a U.S. person possessing/distributing preteen CP. Requiring a conviction would tend to prevent the Cobra Effect of a reward making the problem worse (e.g., increasing the production of preteen CP so that tipsters

[169] International Centre for Missing and Exploited Children, *Powering the Search for Missing Children*, https://www.icmec.org/support-us/impact/.

can collect a reward for reporting).[170] Further, the problem of increased online offerings of CP to U.S. persons may develop if offerors can collect a reward by providing a tip that convicts the recipient for receipt). A tipster program could be operated by NICMIC and/or other public or private entities to financially incentivize reporting of child pornography involving young victims. A tipster reward program can be funded by private donors or through taxation, particularly donations by or taxes imposed on tech platforms providing warrant proof encryption.

An anonymous tipster reward program could be feasible, if it might increase reporting among witnesses reluctant to transparently report, but such a program would need appropriate technical and administrative safeguards to facilitate anonymity. An example of a private anonymous crime reporting system based out of California is https://wetip.com/ This organization has an infrastructure to support rewards for anonymous crime reporting (but it does not solicit reports of child pornography). Advertising of a tipster program could be provided on social media platforms or elsewhere, such as in schools.[171] The question is whether an anonymous private crime reporting system for child pornography is feasible in terms of how important is it for a reporting party to identify herself? Certainly, one risk might involve false reporting in

[170] For a general description of the Cobra Effect, See Cobra Effect, Wikipedia, https://en.wikipedia.org/wiki/Cobra_effect (last updated March 12, 2021)(describing the Cobra Effect as occurring "when incentives designed to solve a problem end up rewarding people for making it worse. The term is used to illustrate how incorrect stimulation in economics and politics can cause unintended consequences. It is also known as the perverse incentive. The term *cobra effect* originated in an anecdote that describes an occurrence during India under British Rule. The British government was concerned about the number of venomous cobras in Delhi. The government therefore offered a bounty for every dead cobra. Initially, this was a successful strategy; large numbers of snakes were killed for the reward. Eventually, however, enterprising people began to breed cobras for the income. When the government became aware of this, the reward program was scrapped. When cobra breeders set their now-worthless snakes free, the wild cobra population further increased."

[171] The Thorn report, discussed above, identifies schools as a helpful institution for intervention with regard to sex trafficking of minors; thus, schools might also be helpful institutions for detecting victims of CP.

order to harm another person's reputation or subject that person to an unfounded investigation (a concept similar to the swatting phenomenon that law enforcement regularly faces).[172] Another hurdle that might need to be cleared is whether the organization is authorized to solicit the public for illegal content to be used as evidence without violating the CP statute.

3. Licensing of Private Researchers to Corroborate Law Enforcement Claims

The number of preteen CP that occurs across the world is severely underreported. In the early 2000s, almost a hundred countries around the world either had no laws addressing child pornography or inadequate laws addressing CP.[173] By 2012, there were still 53 countries that did not have any CP laws.[174] Since 2012 there has not been much improvement in CP laws across the world. The ICMEC has stated the insufficiency of CP laws is a large contributing factor to why the number of CP acts is so large, and likely underreported.[175]

The five criteria required by the ICMEC to be in compliance with ICMEC recommended sufficient CP laws include: having existing laws with a legal definition of CP; making CP a crime;

---

[172] For a general discussion of the swatting phenomenon, *see* 64 DRAKE L. REV. 455 *(2016)*
Swatting: The New Cyberbullying Frontier after Elonis v. United States, Jaffe, Elizabeth M.
(describing "the prankster convinces a police dispatcher to send an entire SWAT team in response to a [fabricated] violent scenario allegedly in progress.").

[173] LifeSite, *New Study Reveals Child Pornography Not a Crime In Most Countries*, LifeSiteNews.com, (Jun. 19, 2021, 11:15 PM), https://www.lifesitenews.com/news/new-study-reveals-child-pornography-not-a-crime-in-most-countries/.

[174] *Id.*

[175] The International Centre for Missing & Exploited Children, *Despite Increase in Global Child Protection Laws Many Countries Still Do Not Consider Child Pornography a Crime*, PR Newswire, (Mar. 26, 2013, 10:00 AM), https://www.prnewswire.com/news-releases/despite-increase-in-global-child-protection-laws-many-countries-still-do-not-consider-child-pornography-a-crime-200036181.html.

whether or not distribution of CP via computer and the internet is a crime; making possession of CP a crime; and whether or not ISPs are required to report suspected CP to law enforcement.[176] Of the countries reviewed in the 2012 report, only 22 countries sufficiently met compliance with the recommended sufficient CP laws.[177] Only 69 countries around the world meet at least 4 of the recommended criteria (considered "sufficient laws") including the United States.[178]

Notably, the Western countries are significant players in the proliferation of CP. Germany has been noted as one of the significant makers of child pornography and the most significant disseminating countries include the Netherlands and the United Kingdom.[179] The largest market and countries with CP consumers include the United States and Southeast Asia.[180] With Western countries being the most technologically advanced and capable of combating CP and being significant players in the proliferation of CP, countries like the United States should increase efforts to combat CP.

Considering the lack of consistent global support to prevent CP, there are few other avenues left to try to combat CP. Enlisting private researchers to corroborate law enforcement claims would help these countries which only meet the minimum requirements set by the ICMEC. Enlisting private researchers would also help understand the magnitude of CP crimes and acts happening across the world and within respective countries.

A licensed private researcher system should be established so that independent third-party researchers can corroborate law enforcement's claims regarding the amount and type of CP

[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] Deepa Salian and Sofia Khatun, *Legal Framework on Child Pornography: A Perspective*, Intech Open, (May 28, 2020), https://www.intechopen.com/profiles/320459.
[180] *Id.*

produced annually. Such independent corroboration seems particularly vital given that society is recovering from the narrative concerning the war on drugs (e.g., asserting marijuana as an inescapable gateway to other drugs). Along these lines, it is important for society to have solid data about the extent of CP and what proportion of it involves young pre-teen children versus CP self-produced by sexually active teenagers versus teenagers victimized by a third-party adult.

Corroboration of law enforcement claims is critical in order to have well informed decision making. Essentially, history teaches that law enforcement can offer an exaggerated narrative at times for varying reasons. This article does not suggest that the FBI's claims are false, but instead asserts that independent verification of those claims seems an important safeguard. As noted earlier in the article law enforcement and some authoritarian regimes have been known to fear monger and over exaggerate claims such as those related to marijuana. In 1930, Harry Anslinger was appointed the first commissioner of the FBI whose work set up the framework for the war on drugs and racist ideology surrounding drug crimes.[181] Without corroboration of evidence, work completed by law enforcement may be chasing down unsubstantiated cases and claims. Licensing private researchers to corroborate law enforcement evidence should help address this issue, and care should be taken that any licensed private researchers have the ability and mission to provide objective, unbiased research rather than being paid to provide research results to simply reinforce a particular narrative provided by the government granting the research license.

4. A Private Bounty Hunter System May Not Be Practical but Should Not Be Ruled Out

[181] Cydney Adams, *The man behind the marijuana ban for all the wrong reasons*, CBS News (November 17, 2016, 5:45 PM), https://www.cbsnews.com/news/harry-anslinger-the-man-behind-the-marijuana-ban/#app.

Individuals should continue to explore private solutions to CP because law enforcement cannot fix the problem unless communities opted to become police states. A private bounty hunter system seems less feasible based on law enforcement concerns, such as the credibility of vigilantes when placed on the witness stand. Major problems with a private bounty hunter system may include the following: (1) a Cobra Effect where a bounty system makes the problem worse, (2) legal issues with credibility of a bounty hunter in a criminal prosecution, and (3) potential embarrassment to law enforcement based on deputized private parties having lower ethical standards/less training than experienced law enforcement personnel. However, such a crowd sourced system should not be ruled out.

Another issue is whether law enforcement authorizing a private bounty hunter to hack the perpetrator's system takes the bounty hunter outside of the private search doctrine (and thus would likely require a warrant given that licensure would require a fair amount of law enforcement supervision of a private bounty hunter).[182] Essentially, the licensing of a bounty hunter could make that hunter an agent of the government, which could require the hunter to obtain a warrant in order to hack the perpetrator's identity. This administrative hurdle could slow the bounty hunter's progress, especially if time is of the essence. Perhaps a statutory provision could provide immunity for the hunter's hacking activity upon his verification of CP content or activities.

Regarding licensure of private bounty hunters, various issues should be considered. First, can the license permit a private bounty hunter to solicit the illegal content given that 18 U.S.C.

[182] *See* Andrew MacKie-Mason, *The Private Search Doctrine after Jones*, 126 YALE L.J. F. 326, 326 (2016-2017)(describing the private search doctrine: "once a private party has conducted an initial search independent of the government, the government may repeat that search, even if doing so would otherwise violate the Fourth Amendment. The private party's search renders the subsequent government "search" not a search in the constitutional sense.").

2252A generally prohibits soliciting the material?[183] (Likewise, a federal license would need to exempt prosecution under any relevant state law as well.) Next, assuming bounty hunters were granted this authority to solicit, care should be taken that they are not creating a market for the creation of child pornography; for example, one could imagine a bounty hunter offering one hundred dollars for an image, which then induces someone (say in a third world country) to then sexually abuse a child and record it. Licensure of bounty hunter activities should thus be carefully monitored so as to avoid creating a market or even creating entrapment situations.

Another issue to consider is whether private bounty hunters, upon detecting child pornography, could then be empowered to hack the perpetrator's systems to determine his identity given that the Computer Fraud and Abuse Act generally prohibits unauthorized hacking activity.[184] While passive detection would certainly seem allowable, hacking activity could be problematic in terms of harming innocent bystanders.[185] Henzey proposed in 2011 a strict liability system for hacking suspected CP perpetrators, but the problems of allowing hacking activity by private parties, even licensed private parties, certainly poses some risks of harming innocent bystanders.[186] In addition, a strict liability system would not help innocent victims of the hacking activity if the vigilante lacks the funds to compensate such victims. Allowing private bounty hunters to hack into individuals' computers has multiple

[183] U.S. v. Williams, 553 U.S. 285, 288 (2008)(noting that 18 U.S.C. 2252A(a)(3)(B) "criminalizes, in certain specified circumstances, the pandering or solicitation of child pornography.")

[184] *See* Don Maclean, *The Problems with Hacking Back*, AFCEA International (May 30, 2018), https://www.afcea.org/content/problems-hacking-back (noting that the problems with hacking back may outweigh the perceived benefits because the hacking back activity may harm innocent bystanders).

[185] *Id.*

[186] Michael J. Henzey, *Going on the Offensive: A Comprehensive Overview of Internet Child Pornography Distribution and Aggressive Legal Action*, 11 APPALACHIAN J.L. 1, 67 (2011)(suggesting that applicable law should "make the hacker strictly liable if she misidentifies as a target someone who is not engaged in trafficking child porn.").

potential liability issues. The hacker may not be able to effectively locate a perpetrator and consequently hack an innocent bystander which may lead to destruction of the innocent bystander's files and data systems or other unintended consequences.[187] With the proper safeguards and support to hackers serving to locate CP and perpetrators, some of these consequences and need for compensation could be addressed.

The feasibility of such a system could be further explored, particularly if data suggests that a large number of preteens are being victimized in CP, and if law enforcement could build a successful, prosecutable investigation based on crowdsourced bounty hunting activity. A private crowdsourced enforcement option could be a highly effective deterrent, but it would first require corroboration of law enforcement's narrative and then it would need to be designed in such a way that it would avoid doing more harm than good (e.g., avoid criminal CP solicitation violations or harmful offensive hacking activity by well-intentioned vigilantes).

There are organizations that team up with law enforcement to help with community policing and regulation. An example of such an organization is InfraGard which is a partnership between the FBI and members of the private sector to provide protection for the U.S. Critical Infrastructure.[188] The competing interests of communities and law enforcement of privatizing law enforcement and protecting communities creates friction between the two parties. This friction sets up a question that communities must decide: should privatization of security and law enforcement roles be a primarily government function? Considering this friction and the question faced by communities, a private bounty hunter system should be considered.

Other well-known examples include Google and Facebook collaborating with law enforcement. A further example includes the private entity Thorn developing its Spotlight software with free

[187] Don Maclean, *The Problems with Hacking Back*, AFCEA International, (May 30, 2018), https://www.afcea.org/content/problems-hacking-back.
[188] InfraGard, Partnership for Protection, https://www.infragard.org/.

access by law enforcement to facilitate child trafficking investigations (with some quotes from law enforcement praising its helpfulness on Thorn's site).[189] It would seem that exploration of financial incentives for private entities (and conceivably individual private actors) might further inspire private parties to combat online CP (beyond purely altruistic motives).

5. Courts Could Consider Allowing Compelled Production of a Defendant's Password or Decryption Key as a Deterrent to CP, but this may Violate the Fifth Amendment

As a final thought, additional courts could hold that defendants can be compelled to turn over their decryption key or password (i.e., pursuant to a warrant) under appropriate circumstances without violating the Fifth Amendment, treating the password as equivalent to a physical key rather than self-incriminating testimony. From a policy standpoint, this would seem a fair compromise in terms of generally respecting privacy of consumer data but allowing for a judicial order to access a suspect's data in the face of probable cause that CP is on the machine. Such a balance avoids the many problems of mandating a decryption back door, and courts may consider invasive electronic searches only where serious suspected crimes are at issue (e.g., felonies such as CP) based on evidence supporting a high likelihood of defendant committing the crime. Along these lines, courts might lean toward denying requests for invasive searches where certain low-level misdemeanor crimes are suspected (e.g., perhaps illegal gambling or ordinary prostitution), but override privacy concerns where more serious CP criminal activity is suspected. Certainly, the Supreme Court has historically allowed special Fourth Amendment exceptions for officer safety and for schools.[190] (Granted, searching a minor seems different from searching an adult.) So, perhaps a Fifth Amendment exception could be explored where compelled password protection is allowable in the limited context of CP?

[189] Thorn, https://spotlight.thorn.org/about

[190] For some historical context of searches in schools, See Stuart C. Berman, Student Fourth Amendment Rights: Defining the Scope of the T.L.O. School-Search Exception, 66 N.Y.U. L. REV. 1077 (1991).

However, this may not be feasible as the Fifth Amendment is a powerful constitutional protection even where the most serious crimes are at issue (e.g., even a murder charge does not justify compelled self-incriminating testimony).

As of this writing, SCOTUS has declined certiorari on the issue of compelled password production in the criminal context. The majority of lower courts agree that sharing a password with law enforcement is a testimonial act because it compels information from a person's mind.[191] Where the courts and scholars disagree, however, is in cases where the suspect is compelled to unlock a device without communicating the password, whether the foregone conclusion doctrine applies to the password itself, or the documents and files the password protects. Some courts, like the majorities in *Commonwealth v. Davis* and *Pollard v. State* are hesitant to apply the foregone conclusion doctrine to the password, and not the phone's files, without express guidance from the Supreme Court.[192] Others, like the dissent in *Davis*, or the court in *State v. Andrews*, find that the foregone conclusion test applies to the production of

[191] Pollard v. State, 287 So. 3d 649, 653 (Fla. Dist. Ct. App. 2019) ("Forcing a defendant to disclose a password, whether by speaking it, writing it down, or physically entering it into a cellphone, compels information from that person's mind and thereby falls within the core of what constitutes a testimonial disclosure."); State v. Andrews, 234 A.3d 1254, 1273 (2020), *cert. denied*, 141 S. Ct. 2623 (2021) ("A cellphone's passcode is analogous to the combination to a safe, not a key. Communicating or entering a passcode requires facts contained within the holder's mind -- the numbers, letters, or symbols composing the passcode. It is a testimonial act of production."); Commonwealth v. Davis, 220 A.3d 534, 548 (2019) ("Based upon these cases rendered by the United States Supreme Court regarding the scope of the Fifth Amendment, we conclude that compelling the disclosure of a password to a computer, that is, the act of production, is testimonial."); United States v. Spencer, No. 17-CR-00259-CRB-1, 2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018) ("For instance, the government could not compel Spencer to state the password itself, whether orally or in writing.").

[192] Commonwealth v. Davis, 220 A.3d 534, 550 (2019); Pollard v. State, 287 So. 3d 649, 656 (Fla. Dist. Ct. App. 2019).

the passcodes themselves, rather than to the phones' contents.[193] SCOTUS declined certiorari in *State v. Andrews*, leaving the exactness of the foregone conclusion doctrine for password compulsion unsettled law.

As courts grapple with this issue, they will likely continue to ponder the words of Justice Stevens from his dissent in *Doe v. U.S.*: "A defendant can be compelled to produce material evidence that is incriminating. Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will. But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe—by word or deed."[194]

In deciding whether and to what extent a Fifth Amendment exception could be carved out in the CP context, courts will certainly consider a variety of factors, such as the likelihood of defendant engaging in the alleged activity based on the strength of evidence, the minimal independent testimonial value of the password itself, the necessity of compelling disclosure given society's interest in protecting vulnerable children, the ability or lack of ability to obtain the evidence by other means, the likelihood of such compelled disclosure being used as a pretext for detecting crimes unrelated to CP, and whether there might be a lower expectation of privacy where the government discovers that defendant has communicated with or about minors in an inappropriate way. Perhaps courts might consider whether compelling the password's production in a particular case would support the government's ability to engage in fishing expeditions against a broad swath of individuals or instead seems based on

[193] Commonwealth v. Davis, 656 Pa. 213, 248 (2019) (Baer, J., dissenting); State v. Andrews, 243 N.J. 447, 478 (2020), *cert. denied*, 141 S. Ct. 2623 (2021).
[194] Doe v. U.S., 487 U.S. 201, 219 (U.S.1988).

strong suspicion targeting one criminal defendant in appropriate circumstances?

CONCLUSION

The foregoing is intended to stimulate further discussion regarding strategies to combat proliferation of CP given that law enforcement may never have a mandatory legislative encryption back door. The tension between privacy interests and the need to combat terrorism, CP, and other serious crimes will continue to exist far into the future. Certainly, technology has created new avenues for perpetrators to hide behind or for innocent actors to maintain strong privacy. Policy makers will continue to struggle with the question of where to draw the line between protecting privacy in society while detecting and preventing serious crimes. Providing law enforcement with too much power would resemble a society policed by an authoritarian regime. However, a free society making no significant attempt to detect and prevent serious crimes against children would be repulsive.