350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: 212-290-4700
Fax: 212-736-1300; 917-591-3452

HUMAN RIGHTS WATCH

HRW.org

Matt Dummermuth
Principal Deputy Assistant Attorney General
US Department of Justice
810 Seventh St. NW
Washington, DC 20531

Cc: Caren Harp
Administrator, Office of Juvenile Justice and Delinquency Prevention
US Department of Justice

Michael Horowitz
Inspector General
US Department of Justice

Peter Winn
Acting Chief Privacy and Civil Liberties Officer
US Department of Justice

Re: Child Protection System software suite

February 1, 2019

Dear Mr. Dummermuth:

We write to ask questions and express concerns about Child Protection System (CPS), a software suite that federal and state law enforcement—including members of the Internet Crimes Against Children Task Force Program established by the Justice Department—use to investigate crimes related to the sharing of child sexual exploitation images.

Human Rights Watch has long promoted accountability for sexual abuse of children around the world, and recognizes that lawful and rights-protecting efforts to prosecute and punish those who commit such crimes are of utmost importance.[1] Our examination of CPS, however, raises several concerns that tie into broader problems in the US criminal justice system.

Specifically, we are concerned that:

[1] Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and pornography, UN Doc. A/RES/54/263 (March 16, 2001), art. 3(1)(c), https://www.ohchr.org/en/professionalinterest/pages/opsccrc.aspx (accessed October 29, 2018). Human Rights Watch has produced a substantial body of work investigating and advocating effective measures to curb sexual abuse of children. Some examples include Human Rights Watch, *Breaking the Silence: Child Sexual Abuse in India* (2013), https://www.hrw.org/report/2013/02/07/breaking-silence/child-sexual-abuse-india; Human Rights Watch, "End Child Marriage," https://www.hrw.org/EndChildMarriage; and Saroop Ijaz, "Protect Pakistan's Children from Sexual Abuse," commentary, Human Rights Dispatch, August 14, 2018, https://www.hrw.org/news/2018/08/14/protect-pakistans-children-sexual-abuse.

- As has proven to be the case regarding other technical investigative methods US authorities have previously employed,[2] the CPS software may not have been subject to thorough independent testing of its accuracy and functioning. Since the system is designed to flag people as suspected of having committed crimes, both its error rates and its potential to exceed constitutional bounds have implications for rights. It is unclear what information the Justice Department has about CPS' potential for error (and on what basis), although prosecutors stated in one court filing that CPS mistakes are "practically nonexistent."[3]
- CPS is provided by a non-profit organization that has repeatedly stated it offers the system exclusively to law enforcement, while prosecutors have argued that they cannot provide the software to criminal defense experts for testing because it is proprietary and not in the government's possession. We fear that the government may be shielding its methods from scrutiny by relying on its arrangements with the non-profit—one whose close relationship with police may, in fact, make it a government agent.
- The CPS software may be facilitating undisclosed police access, without legal process, to personal data about internet subscribers held by a datamining program that private credit reporting agency TransUnion owns. There appears to be a close relationship between the non-profit organization that offers CPS and this private credit reporting agency. If this is indeed occurring, such a practice would give rise to constitutional, federal, and human rights law and policy concerns.
- Among the potential issues arising from any such secret law enforcement access to personal data is that defendants and trial courts may not learn about, or be able to challenge, the breadth of information police obtain—and the potential for that information to facilitate decision-making based on implicit bias or other improper factors.
- Law enforcement may be concealing any such secret use of personal data by deliberately creating a new and different paper trail—a practice known as "parallel construction," which our prior reporting suggests is a common and rights-harming problem in US prosecutions.[4]
- Potential errors by officers in identifying files as illicit—and registering them as such in a shared database—may harm legitimate free expression in a lasting manner. It is unclear whether any systematic review occurs to prevent this from happening.
- The available sources do not indicate what efforts the Justice Department or other law enforcement agencies make to ensure that any data incorrectly linking innocent people to the highly stigmatized offense of possessing child sexual abuse images is corrected or deleted.

This letter provides background and details regarding these concerns and seeks information from the Justice Department on or before February 18, 2019 about current policies and practices related to law enforcement uses of CPS.

---

[2] Recent examples include hair comparisons and bite-mark analysis. See, for example, President's Council of Advisors on Science and Technology, *Forensic Science in Criminal Courts: Ensuring the Scientific Validity of Feature-Comparison Methods* (2016), pp. 8-9, 13-14, 83-87, 118-122, https://www.innocenceproject.org/wp-content/uploads/2017/03/PCAST-2017-update.pdf (accessed October 30, 2018) (hereinafter "PCAST Report").

[3] *Infra* n. 22 and accompanying text.

[4] Human Rights Watch, *Dark Side: Secret Origins of Evidence in US Criminal Cases*, January 2018, https://www.hrw.org/sites/default/files/report_pdf/us0118.pdf.

The discussion below is based on research we conducted between May 2016 and October 2018, including an examination of records from 20 federal prosecutions in which the government explicitly disclosed the use of CPS, as well as information appearing in a set of federal civil-rights lawsuits brought against local authorities in Mississippi in 2011 following the use of CPS there. (See Appendix for a list of these cases.) Although we do not address state cases here, media coverage and other sources suggest that prosecutions in state courts involving CPS use may be common.[5]

The CPS Software Suite

CPS is a set of software tools and databases designed to help law enforcement identify individuals who allegedly share child exploitation images on peer-to-peer networks, which enable internet users to connect to one another and trade files such as pictures, music, and videos. A US-based non-profit organization, Child Rescue Coalition (CRC), reports that it provides the software suite to law enforcement—including the Internet Crimes Against Children Task Force run by the Justice Department.[6]

It is our understanding that a CPS component called Peer Spectre monitors file-sharing traffic on peer-to-peer networks. Anyone on a peer-to-peer network can search for files by keyword, and we understand that Peer Spectre carries out continuous, automated keyword searching for suspicious file titles and identifies Internet Protocol (IP) addresses that are allegedly sharing those files. The results of these searches are logged in servers law enforcement can access.

We understand that a second component of CPS, Shareaza LE, then enables law enforcement to single out a particular IP address and attempts to download all the files it is sharing, a technique known as a "sole source download." This gives police a means of investigating the tips CPS generates when it monitors the peer-to-peer network. Our information suggests that without Shareaza LE (which is not available to the public), peer-to-peer network users typically cannot carry out sole source downloads.

We understand that at these initial stages, suspected child exploitation images are identified using "hash values," or unique digital identifiers roughly analogous to fingerprints, that can be calculated for many files using certain algorithms.

What is now CPS was apparently developed as part of a collaborative effort by law enforcement authorities and then was acquired by a data broker known as TLO, LLC, in

[5] See, for example, Carey Codd, "Boca Raton-Based Child Rescue Coalition Works 'To Find Those That Victimize Kids,'" *CBS4 News*, November 18, 2015, https://miami.cbslocal.com/2015/11/18/boca-raton-based-child-rescue-coalition-works-to-find-those-that-victimize-kids/ (accessed December 12, 2018) ("The Broward State Attorney's Office said they've prosecuted close to 150 cases based on information supplied by the Child Rescue Coalition"); *People v. Worrell*, 59 Misc. 3d 594 (N.Y.), March 2, 2018; *State v. Baric*, 2018 WI App. 63 (Wis. Ct. App.), September 18, 2018; *Frazier v. State*, 180 So. 3d 1067 (Fla. Dist. Ct. App.), November 20, 2015.

[6] *United States v. McKinion*, no. 2:14-cr-00124 (C.D. Cal..), Declaration of William S. Wiltse (doc. 62-1), para. 2; Child Rescue Coalition Inc., Internal Revenue Service Form 990 (2017), p. 36; Department of Justice, "Office of Juvenile Justice and Delinquency Prevention's Internet Crimes Against Children Task Forces Arrest More Than 1,000 Child Predators in Operation Broken Heart," Press release, June 22, 2015, https://www.justice.gov/opa/pr/office-juvenile-justice-and-delinquency-prevention-s-internet-crimes-against-children-task (accessed October 30, 2018); Internet Crimes Against Children Task Force Program, https://www.icactaskforce.org/ (accessed October 30, 2018).

2009.[7] TLO was purchased by credit reporting agency TransUnion in 2013 after filing for bankruptcy and is now known as TLOxp.[8] CRC, the non-profit organization that now offers CPS, was established in the wake of TLO's bankruptcy and continues to share a physical address with TLOxp.[9]

Reliability Testing Concerns: Accuracy and Reach

1. Accuracy

Concern has grown in recent years about how US courts regard technical investigative methods and whether those methods have been adequately tested to ensure their accuracy and consistency.[10] Without rigorous testing, it is impossible to know objectively how often an investigative method produces false positives or false negatives, and what factors may affect those rates.[11]

However, to date we have not found any public information on CPS having been tested by qualified independent experts or results of such testing.

Knowing the accuracy of investigative methods is important for human rights and constitutional reasons. Except in an emergency or other exceptional circumstance, US police may force people to submit to intrusive searches of their homes or electronic devices only if the authorities first obtain a warrant from a court based on a demonstration that they have probable cause to believe they will find evidence of a crime. To show that such probable cause exists, they may rely wholly or partly on results from an investigative tool such as CPS. If the tool has accuracy problems, its results may not provide a sufficiently sound basis for a court to include in the justification for issuing a warrant—and a warrant issued without probable cause is unconstitutional under the Fourth Amendment. In turn, under the "fruit of the poisonous tree" rule, trial courts will normally prohibit prosecutors from introducing any evidence that derives from an initial illegal search, such as one based on a warrant that lacked probable cause.[12]

---

[7] See, for example, *United States v. Dang*, no. 6:16-cr-10027 (D. Kan.), Affidavit of William S. Wiltse (doc. 23-1), undated, filed September 26, 2016, para. 2; *United States v. Clements*, no. 1:15-cr-00275 (N.D. Ohio), Affidavit of William S. Wiltse (doc. 18-1), August 2, 2013, para. 2.

[8] Jeff Ostrowski, "After founder's death, Boca tech firm TLO files for Chapter 11," *Palm Beach Post*, May 9, 2013, https://www.mypalmbeachpost.com/business/after-founder-death-boca-tech-firm-tlo-files-for-chapter/34CcCzHza646WkCtWoWZuN/ (accessed October 30, 2018); TransUnion, "TransUnion Completes Acquisition of TLO," https://newsroom.transunion.com/transunion-completes-acquisition-of-tlo/ (accessed October 30, 2018); TransUnion and TLOxp, www.tloxp.com (accessed October 30, 2018).

[9] CRC's Form 990 tax filing for 2013 covers a period beginning December 11, 2013, suggesting that the organization was established on or around this date. Its address is listed on its 2017 Form 990; the same address is listed on TLOxp's "Contact Us" page, https://www.tlo.com/contact (accessed October 31, 2018).

[10] See, PCAST Report, *supra* n. 2, pp. 3-6; Rebecca Wexler, "Convicted by Code," *Slate*, October 6, 2015, https://slate.com/technology/2015/10/defendants-should-be-able-to-inspect-software-code-used-in-forensics.html (accessed October 31, 2018); Jonathan Jones, "Forensic Tools: What's Reliable and What's Not-So-Scientific," Frontline, April 17, 2012, https://www.pbs.org/wgbh/frontline/article/forensic-tools-whats-reliable-and-whats-not-so-scientific/ (accessed October 30, 2018); Innocence Project, "Misapplication of Forensic Science," undated, https://www.innocenceproject.org/causes/misapplication-forensic-science/ (accessed October 30, 2018).

[11] See generally PCAST Report, *supra* n. 2, pp. 5-6.

[12] *Wong Sun v. United States*, 371 U.S. 471 (1963).

This means establishing a technique's error rates is critical both to protecting people from unconstitutional searches and to ensuring that in a criminal trial, the prosecution cannot unfairly benefit from illegal police activities.

Where software is concerned, the Justice Department's policy guidance states that such tools "used to support evidence discovery, extraction and examination, case examination and evaluation and method development shall be technically reviewed by qualified experts and validated prior to use."[13] Materials the US Commerce Department's National Institute of Standards and Technology (NIST) has published help demonstrate that it is possible to develop a methodology for objectively testing how, and how reliably, software operates. For example, as part of a project concerning computer forensic tools, NIST has set out a testing process that includes, inter alia:

- The development of test cases, which are then posted online, along with other information, for "peer review by members of the computer forensics community and for public comment by other interested parties";
- The incorporation of feedback from the peer-review and public-comment processes;
- NIST's acquisition of the tool for testing;
- An examination of the available documentation;
- The selection of appropriate test cases;
- The development of a test strategy;
- The execution of the test; and
- The production and online posting of a test report.[14]

As noted above, despite the existence of such scientific methodologies and the Justice Department's policy, we have been unable to locate any evidence that CPS has been subjected to complete, independent, peer-reviewed testing. If such tests have been carried out, we request that you make the studies publicly available.[15]

When defendants have made motions seeking to arrange for expert testing of the software, federal prosecutors have sometimes sought to avoid producing CPS' source code for testing on the grounds that it is protected from disclosure by law enforcement privilege,[16] that the code is proprietary and not in the government's possession[17]—or both.[18] We have identified only one case—*United States v. Ocasio*—in which prosecutors ultimately produced the CPS

[13] U.S. Department of Justice, "Scientific Research and Integrity Policy," undated, https://www.justice.gov/olp/forensic-science (accessed December 6, 2018), p. 6.
[14] National Institute of Standards and Technology, "Methodology Overview," February 22, 2018, https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt/cftt-general-o (accessed October 30, 2018).
[15] CRC's president William Wiltse testified during a 2013 hearing concerning a defense motion to suppress in *United States v. Thomas*, a Vermont federal case, that some aspects of the CPS suite were tested internally to a certain degree when CPS was first developed, but that the suite had not been tested more recently or subjected to thorough, independent testing using a standardized process. *United States v. Thomas*, no. 5:12-cr-00037 (D. Vt.), "Transcript: Motion to Suppress & Request for a *Franks* Hearing," (doc. 99), April 17, 2013, pp. 102-110.
[16] See, for example, *United States v. Dang*, *supra* n. 7, Response to Defendant's Motion to Compel Production (doc. 23), September 26, 2016, p. 12; *United States v. Hartman*, no. 8:15-cr-00063 (C.D. Cal.), Opposition to Defendant's Motion to Compel Discovery (doc. 37), September 24, 2015, p. 4.
[17] See, for example, *United States v. Neale*, no. 5:12-cr-00044 (D. Vt.), Response to Defendant's Motion to Compel Discovery (doc. 44), December 7, 2012, pp. 8-10; *United States v. Crowe*, no. 1:11-cr-01690 (D.N.M.), Response to Defendant's Motion to Compel and Motion to Inspect (doc. 58), June 1, 2012, pp. 11-15.
[18] *Ibid.*; *United States v. Dang*, *supra* n. 7, Response to Defendant's Motion to Compel Production (doc. 23), September 26, 2016, pp. 12, 23-24.

source code to a defendant, and a statement submitted in a later case suggests that *Ocasio* was resolved through a plea agreement before any expert testing took place.[19]

By contrast, in a 2015 decision in *United States v. Naylor*, a West Virginia federal court simply accepted an officer's assertion that in his personal experience, the tool had never erred and was (in the court's words) "100% reliable."[20] The court therefore concluded that "[t]he CPS software appears to be a reliable investigative tool for law enforcement in these types of cases" and rejected the defendant's motion to suppress evidence found through the software.[21] In at least one case, the government itself has asserted in a motion that "[e]rror is practically nonexistent in the Shareaza LE and CPS systems" without citing any sources for this claim.[22]

We fear this situation—in which prosecutors resist defense testing of CPS but are willing to make, or apparently allow witnesses to make, assertions about the software's accuracy—may interfere with the judiciary's ability to assess the tool's potential for malfunction, and thus jeopardize fair-trial rights.

Regarding assertions that CPS' source code is proprietary or otherwise not in the government's possession, we note that CRC has consistently described itself as heavily enmeshed with and dedicated to furthering the operations of law enforcement. In its tax filings, the organization has stated that it "offers space at its operational location to law enforcement agencies in order to easily access the tracking system."[23] Affidavits by the group's president, William Wiltse, have described access to CPS as "made available to specifically trained and licensed law enforcement officers and … *restricted to only those law enforcement officers in the performance of law enforcement activity*" (emphasis added).[24] Testimony by Wiltse in 2013 concerning CPS-enabled investigations (prior to the establishment of CRC) described a "restricted area" on TLO's property: "The only people allowed into this area are sworn law enforcement officers. Even our boss, our CEO, cannot get into this area without being escorted," Wiltse told the court.[25] Wiltse himself is a reserve deputy sheriff for Florida's Palm Beach County, according to his affidavits and CRC's website.[26]

---

[19] For the decision granting the defendant's motion to compel production of the CPS source code in *United States v. Ocasio*, no. 3:11-cr-02728 (W.D. Tex.), see 2013 U.S. Dist. Lexis 79313 (2013 WL 2458617), June 6, 2013. For a discussion concerning how *Ocasio* was resolved, see *United States v. Shia*, no. 3:15-cr-00257 (N.D. Cal.), Affidavit of Tami Loehrs Re Ocasio Case (doc. 27), November 19, 2015.

[20] *United States v. Naylor*, 99 F. Supp. 3d 638, 643 (S.D.W. Va., 2015).

[21] *Ibid*.

[22] *United States v. Pirosko*, no. 5:12-cr-00327 (N.D. Ohio), Response in Opposition to Defendant's Motion to Compel (doc. 32), August 2, 2013, pp. 7-8. To the best of our knowledge, the case the government mentioned in the second part of the sentence involved a different software program.

[23] See, for example, Form 990 (2017), *supra* n. 9, p. 36.

[24] *United States v. Dunning*, no. 7:15-cr-00004 (E.D. Ky.), August 26, 2015, Affidavit of William S. Wiltse (doc. 30-1), September 14, 2015, para. 13; *United States v. Crowe*, *supra* n. 17, Affidavit of William S. Wiltse (doc. 58-1), June 1, 2012, para. 3; *United States v. Clements*, *supra* n. 7, Affidavit of William S. Wiltse (doc. 18-1), August 2, 2013, para. 3.

[25] *United States v. Thomas*, *supra* n. 15, Transcript, pp. 131-32.

[26] *United States v. Dunning*, *supra* n. 24, Affidavit of William S. Wiltse, para. 1; Child Rescue Coalition, "Our Team," https://childrescuecoalition.org/our-team/ (accessed October 31, 2018).

We therefore regard government arguments that prosecutors cannot produce the CPS source code for testing as both inappropriate and jeopardizing fair-trial rights, insofar as access to the source code is necessary for scientifically sound testing.[27]

2. Reach

Accuracy is not the only aspect of CPS that is susceptible to testing and should be subject to scientifically sound validation prior to law enforcement use. The software suite's reach also has potential constitutional consequences.

Federal courts have found that police do not need a search warrant to monitor peer-to-peer network activities that take place in public,[28] and CRC's president has maintained that the CPS software only locates information that peer-to-peer network users have publicly shared.[29] If this description of CPS is correct, then under current US constitutional law, police may use or rely on the software without obtaining a warrant first.

However, defendants in several federal cases have offered evidence that files (or traces of files) officers have identified using CPS may have been stored in areas of their devices that were not publicly shared, raising Fourth Amendment concerns.[30] We acknowledge that the strength of this evidence is open to debate and that federal prosecutors have challenged the credibility of the forensic expert who produced the relevant reports. However, nowhere in the records we reviewed does the government actually set out evidence refuting the claims that CPS can reach beyond publicly shared folders, let alone persuasively show that the software cannot do so or is not being so used.[31]

This, too, is a matter that rigorous independent testing can and should resolve.

Free Speech and Related Concerns

To function accurately, CPS depends not only on the correct identification of IP addresses and the hash values of shared files, but on police officers correctly designating files as containing illegal child exploitation images. The potential for mistakes in this respect prompts concerns about the resulting impact on legitimate free expression, particularly if the Justice Department does not ensure that these designations are regularly reviewed.

---

[27] See, also, Rebecca Wexler, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System," *Stanford Law Review*, vol. 70 (May 2018), pp. 1364-65, 1429, https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/06/70-Stan.-L.-Rev.-1343.pdf (accessed October 31, 2018) (specifically addressing the CPS case *Ocasio* and concluding that "extending the [trade secret] privilege wholesale from civil to criminal proceedings is both harmful and unnecessary").

[28] See, for example, *United States v. Thomas*, 2013 WL 6000484 (D. Vt. 2013), 47-51 (aff'd 2d Cir., 788 F. 3d 345, 351 (2015); *United States v. Baalerud*, 2015 WL 1349821 (W.D.N.C. 2015), pp. 23-26; *United States v. Dodson*, 960 F. Supp. 2d p. 689, pp. 695-696 (W.D. Tex. 2013).

[29] See, for example, *United States v. Clements*, *supra* n. 7, Affidavit of William S. Wiltse (doc. 18-1), August 2, 2013, para. 8; *United States v. Crowe*, *supra* n. 25, Affidavit of William S. Wiltse (doc. 58-1), May 31, 2012, para. 6.

[30] *United States v. Clements*, *supra* n. 7, Affidavit of Tami Loehrs (doc. 17-2), November 19, 2015, para. 10; *United States v. Crowe*, *supra* n. 25, Affidavit of Tami Loehrs (doc. 48-1), April 26, 2012, paras. 11, 14-16; *United States v. Dang*, *supra* n. 7, Affidavit of Tami Loehrs (doc. 19-1), August 9, 2016, para. 11; *United States v. Hartman*, *supra* n. 24, Affidavit of Tami Loehrs (doc. 50-1), October 8, 2015, paras. 14-16.

[31] See, for example, *United States v. Hartman*, *supra* n. 16, Order Re Pretrial Motions (doc. 87), November 24, 2015, pp. 22-23 (noting that "the Government has not refuted the defense expert's analysis that suggests the files at issue here were not designated as shareable," although it had had "ample opportunity to do so").

An affidavit by Wiltse in an Ohio federal prosecution, *United States v. Clements*, and his 2013 testimony in *Thomas* indicate that officers using CPS may designate newly discovered files as "Child Notable" based on their own opinions and proceed to register hash values for those files in one or more of the system's networked databases.[32] Wiltse's testimony in *Thomas* further indicates that CPS' reliance on these officer-made designations is extensive.[33] However, the records we have examined do not disclose any systematic safeguards for ensuring that these designations are accurate. This raises concerns that people's right to access and receive information—part of the right to free expression—could be at risk if officers mischaracterize files, or generate records when someone possesses lawful files (such as legal adult pornography).

Additionally, we understand that the element of the software suite called Shareaza LE gives officers the technical ability to view the hash values of, and download, *any* file an IP address is sharing on a peer-to-peer network—regardless of whether those files are believed to be illicit.[34] The Justice Department should explain whether it takes steps to ensure officers are not monitoring legitimate free expression in a manner that would be inconsistent with rights laws or policies.

Personal Data and Discrimination Concerns

Through our research, we have become aware of potential law enforcement access to personal information when using CPS. This potential for access could undermine privacy and consumer protections found in federal law, reduce defendants' ability to learn about and challenge any abusive practices, and facilitate improper decision-making.

An undated user agreement for the CPS software submitted as evidence in a 2015 California criminal prosecution, *United States v. Hartman*, suggests that CPS users have—or have had—free access to "Unconfirmed Subscriber Data provided by TLO."[35] "Subscriber" is apparently a reference to people who subscribe to internet services and therefore are associated with an IP address, while "TLO" is a reference to the datamining operation now known as TLOxp.

---

[32] *United States v. Clements*, *supra* n. 7, Affidavit of William S. Wiltse, para. 9 ("The term 'Child Notable' is an *investigator assigned* category for certain file hashes within the Child Protection System…. During training investigators are provided software, which generates hash values for recently located child exploitation files and submits those hash values to CPS databases *with a category selected by the investigator*" (emphasis added)); *United States v. Thomas*, *supra* n. 23, Transcript, pp. 56-57 ("[L]aw enforcement has been aware and continues to become aware of new pieces of child pornography that are being made available on these [peer-to-peer] file sharing networks…. What law enforcement is trained to do is submit the hash values, so we actually give them tools that calculate the hash value for these files, but then law enforcement can then electronically submit those hash values to us, along with a category that the officer is trained to use as far as what is it that this file is categorized as based on your training, and then we then can leverage that hash value or the knowledge of that hash value in programs such as Peer Spectre. So what I mean by that is Peer Spectre is aware of hundreds of thousands of pieces of what *investigators describe as* child notable, which I guess for all intents and purposes is child pornography" (emphasis added))."

[33] *United States v. Thomas*, *supra* n. 23, Transcript, pp. 56-57 ("Peer Spectre is aware of *hundreds of thousands* of pieces of what investigators describe as child notable [files]" (emphasis added)).

[34] See, for example, *United States v. Clements*, *supra* n. 7, doc. 22-6 (filed March 16, 2016); *United States v. Naylor*, *supra* n. 24, no. 2:14-cr-00194 (S.D.W. Va.), doc. 19-1 (filed January 6, 2015), p. 17 of file. These documents are CPS screenshots indicating that officers using the software suite can see that an individual is sharing files that are "Not Categorized," "Adult Erotic," or of "No Known Relevance," in addition to known or suspected "Child Notable" files.

[35] *United States v. Hartman*, *supra* n. 16, "The Child Protection System – Acceptable Use Requirements" (doc. 102-2), undated, filed January 8, 2016, p. 2.

This "Unconfirmed Subscriber Data" might include marketing data about individuals—such as names, telephone numbers, addresses, and dates of birth—that corporate sources have linked to their IP addresses and email accounts. It is our understanding that officers using CPS have been told that no logs will be kept of any search they may perform of this corporate data.

Can you confirm what "Unconfirmed Subscriber Data" includes, from whence it is derived, and the means by which TLOxp could identify IP addresses with specific individuals? We would also like to understand why no records would be kept of law enforcement queries of this data, and whether that is, in fact, the practice.

TLOxp's website indicates that the information the datamining system possesses about an individual may include addresses and phone numbers;[36] records from automated license plate readers,[37] which can reveal where a car has traveled; information from drivers' licenses;[38] Social Security numbers;[39] employment records;[40] social media profiles, including photographs;[41] criminal records;[42] and connections to other people.[43] Please provide your understanding of what types of data CPS users, via TLOxp, may be able to view.

Under the Electronic Communications Privacy Act (ECPA), electronic communications service providers normally may only disclose information identifying the subscriber linked to an IP address in response to a subpoena or other legal process—thus leaving a paper trail defendants can obtain and scrutinize.[44] ECPA also limits the types of subscriber information the provider is obligated to disclose when responding to such a subpoena: primarily name, address, dates and durations of online sessions, and payment information.[45] While ECPA is outdated in many respects and subpoena powers are themselves susceptible to misuse,[46] these provisions nevertheless impose a significant privacy protection and create transparency about both the law enforcement demand and the data disclosed in response to it.

Our understanding is that TLOxp and CRC are not communications service providers and that ECPA therefore does not technically apply to their disclosure of data concerning people linked to IP addresses. However, we are concerned that the use of data from a data broker to identify subscribers without a subpoena or other legal process would subvert the protections Congress intended to establish in the law. Can you provide the details of what types of personal data law enforcement may be able to obtain when using CPS—and whether

[36] TransUnion, "TLOxp for Law Enforcement," https://www.tlo.com/law-enforcement (accessed November 5, 2018).
[37] TransUnion, "TLOxp Vehicle Sightings," https://www.tlo.com/vehicle-sightings (accessed November 5, 2018).
[38] TransUnion, "TransUnion's TLOxp for Law Enforcement," 2017, https://www.tlo.com/resources/tlo/doc/industry/resources/industry-law-enforcement-as.pdf (accessed December 17, 2018), p. 2.
[39] "TLO for Law Enforcement," *supra* n. 36.
[40] *Ibid.*
[41] TransUnion, "TLOxp Social Media Search," https://www.tlo.com/social-media (accessed November 5, 2018); "About TLOxp," *supra* n. 3.
[42] TransUnion, "TransUnion's TLOxp for Law Enforcement," *supra* n. 38, p. 1.
[43] TransUnion, "TLOxp Relationship Report," https://www.tlo.com/relationship (accessed November 5, 2018).
[44] 18 U.S.C. §§ 2702-03.
[45] 18 U.S.C. § 2703(c).
[46] See Human Rights Watch, *Dark Side*, *supra* n. 4, pp. 28-29.

that data may go beyond what a communications service provider would normally disclose under ECPA?

As noted above, TLOxp's technical means of linking individuals to IP addresses also remain unclear. These methods could raise further constitutional or other legal questions when the data is used by law enforcement, rendering the disclosure of information about them desirable to ensure respect for rights. We would appreciate any information you may have as to these technical means, and whether and to what sort of technical or legal review they may have been subjected.

Our understanding of the typical progression of a CPS-enabled investigation is that the software's broad monitoring of peer-to-peer networks results in a database of IP addresses that are suspected of offering illicit files, and that officers can then use a different component of CPS in an attempt to create a complete log of all the files a specific IP address is sharing. At this stage, under ECPA, officers would have the power to issue a subpoena directly to the internet service provider and thereby obtain the name and address of the relevant internet subscriber. Our review of relevant cases suggests that such subpoenas are typically disclosed to defendants, who are then able to review these records. Can you explain why officers may choose to not use the ECPA, which provides a record to courts and defendants, to obtain a defendant's name and address, opting instead to use TLOxp for this purpose?

We further note that CRC's website claims the non-profit offers "[a]nalytics targeting the offenders at greatest risk of presently abusing children."[47] The Justice Department should disclose whether police are receiving the results of such "[a]nalytics," and if so, what data the non-profit uses—or enables officers to use—when making these calculations.

Fundamental Rights Concerns: Parallel Construction

While "Unconfirmed Subscriber Data" from what is now TLOxp appears to be (or have been) available to CPS users, only one case we examined includes a record openly referring to this practice. It is possible that this absence of disclosures is due to officers' decisions not to view or use this data even though CRC has offered it. However, we are concerned that law enforcement may be gaining access to this personal data from or through CRC, and then deliberately concealing how officers obtained the information by re-obtaining it in other ways for use in court—a practice known as parallel construction. In our 2018 report *Dark Side: Secret Origins of Evidence in US Criminal Cases*, we documented evidence suggesting law enforcement has at times used parallel construction to conceal the original sources of leads in some criminal cases.[48]

Parallel construction can prevent courts from reaching important or novel questions about constitutional rights, and defendants from arguing that judges should exclude unconstitutionally obtained evidence under the "fruit of the poisonous tree" rule. The

[47] Child Rescue Coalition, "The Solution," https://childrescuecoalition.org/the-solution/ (accessed December 20, 2018).
[48] Human Rights Watch, *Dark Side*, *supra* n. 4, p. 1.

practice can also prevent defendants from learning that the government obtained exculpatory evidence during its investigation.[49]

As noted above, if police were attempting to obtain the identity of a subscriber associated with an IP address from an internet or telephone service provider, they would need to issue a subpoena.[50] However, the CPS user agreement disclosed in 2016 instructs, "Do not use this [data from TLO] for probable cause. It must be confirmed through other investigative means that are acceptable with your agency and prosecuting attorney."[51] This reference to using "other investigative means" to "confirm[]" personal data previously obtained by another method prompts concerns that officers may employ parallel construction to avoid revealing that their initial leads came from personal data obtained from TLOxp. Can you comment on whether this has been a practice, or whether there are measures to prevent such practices in place?

The potential use of subpoenas as a means of "parallel construction" in a different context is currently the subject of an investigation by the Justice Department's Office of the Inspector General.[52] We encourage the Inspector General, to whom we will send a copy of this letter, to expand its investigation to determine whether such use of subpoenas is occurring in this context as well, and hope you will support such an effort.

In a California federal prosecution, *United States v. McKinion*, a Homeland Security Investigations special agent in Los Angeles used CPS to identify two different IP addresses as allegedly possessing unlawful child sexual abuse images in May 2012.[53] The agent's search warrant application stated that "throughout … April 2012," the agent had "conducted records checks" for McKinion, including searches of address records and employment history.[54] The agent issued either a single subpoena or two subpoenas on the same date to the relevant internet service provider regarding the two IP addresses in May 2012.[55]

In his affidavit, the agent did not explain what databases he used for his "records checks," why he had conducted such checks concerning McKinion in April 2012 if the suspected illicit activities were only detected beginning in May 2012, or whether or how he linked both IP addresses to McKinion prior to issuing the subpoena(s)—especially when one of the IP addresses was shared with seven other people.[56] Likewise, prosecutors did not explain precisely how the two different IP addresses had been linked to the defendant, instead stating simply that the special agent "determined that Suspect IP 1 belonged to defendant and that defendant used Suspect IP 2."[57]

---

[49] *Ibid.* at pp. 3, 57, 59.
[50] 18 U.S.C. § 2703(c)(2).
[51] *United States v. Hartman*, doc. 102-2, *supra* n. 16, p. 2.
[52] Office of the Inspector General, U.S. Department of Justice, "Ongoing Work," https://oig.justice.gov/ongoing/all.htm (accessed November 5, 2018).
[53] *United States v. McKinion*, *supra* n. 6, Affidavit in Support of Search Warrant (doc. 49-2), July 23, 2012, paras. 30-32. **Please be aware that these paragraphs contain graphic and disturbing descriptions of child sexual abuse images.**
[54] *Ibid.* at paras. 35-38.
[55] *Ibid.* at paras. 33-34.
[56] *Ibid.* at para. 34; see also *United States v. McKinion*, *supra* n. 6, Motion to Suppress Evidence Derived from Search Warrant (doc. 47), May 15, 2017, pp. 15-16.
[57] *United States v. McKinion*, *supra* n. 6, Opposition to Defendant's Motion to Suppress Evidence (doc. 49), May 22, 2017, p. 6. The structure of the discussion in this paragraph implies without stating that the special agent made this determination before issuing a subpoena to internet service provider Catalina Computers.

We are concerned that parallel construction may have been employed in this case to avoid the disclosure of investigative activities prior to April 2012 and/or the use of databases that may have linked the IP addresses to individuals' names, and invite the Justice Department to comment on this.

Correcting Mistakes

Human Rights Watch is also concerned about whether CRC or law enforcement delete or correct data incorrectly linking innocent people to the possession of child sexual exploitation materials and, if so, how this is done.

Ensuring the deletion or correction of inaccurate data is essential to respecting rights and dignity. This is especially true when individuals may be wrongly suspected of illicit file-sharing because someone else used their internet services or devices for illegal activities without their knowledge. Police investigations of alleged downloads of child abuse images involving shared wi-fi networks and computers have previously led to questioning and searches impacting innocent people.[58] One such investigation in Jackson, Mississippi in 2011 that involved CPS led to a civil-rights lawsuit against local police.[59]

Wiltse, CRC's president, also acknowledged in a 2017 declaration in *McKinion* that if a malicious hacker gained access to the nonprofit's tools, he or she could "implicate an innocent person's IP address as participating in the collection, manufacture or distribution of child exploitation files."[60] Such a possibility, no matter how seemingly remote, further supports the need for safeguards at all stages in the collection, storage, and sharing of personal data related to such law enforcement activities.

Questions for the Justice Department

In light of the foregoing discussion of concerns, we request that the Justice Department provide answers to the following questions:

Testing

- Has the Justice Department conducted or commissioned thorough independent third-party testing of CPS? If so, what methodology was used and what were the results? If not, does the use of CPS comply with the Department's policy regarding the validation of software tools?

[58] See, for example, *Tuskan v. Jackson County*, *infra* n. 59; Sam Stanton, "He wanted to download child porn, so he hacked his neighbor's wifi," *Sacramento Bee*, August 1, 2017, https://www.sacbee.com/news/local/crime/article164803532.html (accessed December 7, 2018); Anthony Bellano, "Man Was Pirating Neighbor's Wi-Fi To Download Child Pornography: Prosecutor," *Patch*, September 12, 2016, https://patch.com/new-jersey/gloucestertownship/clementon-man-was-pirating-neighbors-wi-fi-download-child-pornography (accessed December 7, 2018); Brett Cihon, "Prosecutor: Man sets up neighbor's Wi-Fi, secretly uses it to download child porn," *Q13 FOX*, April 9, 2014, https://q13fox.com/2014/04/09/prosecutor-man-sets-up-neighbors-wi-fi-secretly-uses-it-to-download-child-porn/ (accessed December 7, 2018); Debra Cassens Weiss, "Prosecutor's Apology for Home Raid Highlights the Dangers of Unprotected WiFi," *ABA Journal*, March 18, 2011, http://www.abajournal.com/news/article/prosecutors_apology_for_home_raid_highlights_the_dangers_of_unprotected_wif/ (accessed December 7, 2018).

[59] *Tuskan v. Jackson County*, 2016 U.S. Dist. Lexis 182700 (S.D. Miss., 2016); for an investigative document showing the use of CPS, see case document 60-9 (case no. 1:13-cv-00356).

[60] *United States v. McKinion*, *supra* n. 6, Declaration of William S. Wiltse (doc. 62-1), October 27, 2017, paras. 15-16.

- Does the Justice Department have policies or practices that relate to the involvement of private or nongovernmental entities in conducting or facilitating law enforcement operations, and if so, what are they?
- What are the Justice Department's policies regarding the level of technical expertise and access to software source code an officer should possess before prosecutors call him or her to testify about the software's functioning and results? Before an officer or agent may attest to the software's results in a search warrant application?
- Does the Justice Department require federal agents to receive training before using CPS? If so, what is the content of this training?

Free Speech

- Has the Justice Department assessed what proportion of files designated as "Child Notable" in CPS or relevant databases constitute unlawful child sexual exploitation images under federal or state law?
- Has the Justice Department analyzed the First Amendment implications of law enforcement use of CPS?

Personal Data and Discrimination Concerns

- Does the Justice Department permit agents to view subscriber data offered by CRC or TLOxp?
- Does the Justice Department believe logs should be kept of law enforcement access to such data? Are such logs kept?
- If agents are permitted to view the data, what types of information are included? What information links individuals' identities to IP addresses, and from what source does that information come?
- Has the Justice Department analyzed whether the protections of the FCRA apply, or should be applied as a matter of policy, to data from TLOxp or CRC? If so, what were the conclusions of this analysis and in what document(s) do they appear?

Parallel Construction

- What are the Justice Department's positions concerning the disclosure of an agent's viewing or use of subscriber data from CRC or TLOxp to courts and defendants? Does the Justice Department require such disclosure if law enforcement subsequently obtains the information in question from other sources?
- Is the Justice Department aware of any use of parallel construction to conceal aspects of investigations involving CPS?
- Does the Justice Department have in place any rule, guidance or measure to prevent or disclose the use of parallel construction in obtaining evidence?

Correcting Mistakes

- What are the Justice Department's policies and practices regarding the identification and treatment of investigative data incorrectly linking an individual, IP address, or device to the possession or sharing of illicit files? What are its policies and practices

regarding whether and how people who may have been wrongly linked to such activities should be notified?
- What are the Justice Department's policies and practices regarding how electronic evidence linking an individual to a suspected offense should be stored and secured? Has the Justice Department determined that CRC is in compliance with these policies, if any?

* * *

We are aware that CPS is not the only software that may be capable of monitoring file-sharing networks for allegedly illegal images, and many of our concerns about this software suite may also apply to other systems. We believe answers to the foregoing questions will assist Congress, the courts, and the public in understanding the Justice Department's treatment of both CPS and other comparable systems, and the broader issues raised by the use of such systems.

We thank you for your attention to this matter and await your response on or before February 18, 2019.

Sincerely,

[signature]

Sarah St.Vincent
Researcher/Advocate on National Security, Surveillance, and Domestic Law Enforcement
Human Rights Watch

Encl.

Appendix: List of federal cases examined by Human Rights Watch

Appendix:
List of Federal Cases Examined by Human Rights Watch

Federal prosecutions

United States v. Baalerud (W.D.N.C., 3:14-cr-00188)

United States v. Brooks (M.D. Fla., 3:13-cr-00058)

United States v. Clements (N.D. Ohio, 1:15-cr-00275)

United States v. Crowe (D.N.M., 1:11-cr-01690)

United States v. Dang (D. Kan., 6:16-cr-10027)

United States v. Dennis (N.D. Ga., 3:13-cr-00010)

United States v. Dodson (W.D. Tex., 4:13-cr-00014)

United States v. Dunning (E.D. Ky., 7:15-cr-00004)

United States v. Hart (W.D. Wash., 3:14-cr-05507)

United States v. Hartman (C.D. Cal., 8:15-cr-00063)

United States v. Juhic (S.D. Iowa, 4:16-cr-00162)

United States v. Leikert (D. Vt., 5:12-cr-00097)

United States v. McKinion (C.D. Cal., 2:14-cr-00124)

United States v. Naylor (S.D.W. Va., 2:14-cr-00194)

United States v. Neale (D. Vt., 5:12-cr-00044)

United States v. Ocasio (W.D. Tex., 3:11-cr-02728)

United States v. Pirosko (N.D. Ohio, 5:12-cr-00327)

United States v. Price (S.D. Fl., 0:12-cr-60016)

United States v. Shia (N.D. Cal., 3:15-cr-00257)

United States v. Thomas (D. Vt., 5:12-cr-00037)

Federal civil actions

Brushaber v. Jackson County, Mississippi et al. (S.D. Miss., 1:13-cv-00453)

Pardue v. Jackson County, Mississippi et al. (S.D. Miss., 1:14-cv-00290)

Peairs v. Jackson County, Mississippi et al. (S.D. Miss., 1:13-cv-00402)

Tuskan v. Jackson County, Mississippi et al. (S.D. Miss., 1:13-cv-00356)