No. 20-50052

---

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

---

UNITED STATES OF AMERICA,

Plaintiff-Appellee,
v.

[redacted]

Defendant-Appellant.

Appeal from the United States District Court
for the Southern District of California
Hon. William Q. Hayes, Presiding
[redacted]

**APPELLANT'S OPENING BRIEF**

Timothy A. Scott
Nicolas O. Jimenez
Scott Trial Lawyers, APC
1350 Columbia Street, Suite 600
San Diego, California 92101
619-794-0451

Attorneys for [redacted]

## Table of Contents

## Table of Authorities

### Cases

**Statutes**

**Other**

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff-Appellee,<br><br>v.<br><br>[redacted]<br><br>Defendant-Appellant. | Case No. 20-50052<br><br>[redacted]<br><br>**APPELLANT'S OPENING BRIEF** |

**Statement of Issues Presented for Review**

**I. Unlawful search and seizure of private online information.**

Private online correspondence and personal information are constitutionally protected. But Yahoo and Facebook secretly monitored their customers' chats and messages, disclosing them (along with other private information) to law enforcement—outside of any judicial process, and in violation of federal statute. Where the F.B.I. had advance knowledge of these unlawful digital searches and acquiesced to them, and the searches were specifically intended to lead to arrests and prosecutions, should the evidence have been suppressed under the Fourth Amendment?

**II. "Purpose" instruction under 18 U.S.C. § 2251.**

For specified sexual conduct to be a crime under 18 U.S.C. § 2251(c), it must be done "*for the purpose* of producing any visual depiction" of said conduct. *Id.* (emphasis added). "For the purpose" is thus a *motive* element, requiring proof that *but-for* that purpose, the act would not have occurred. *See Burrage v. United States*, 134 S. Ct. 881, 888-90 (2014). Where guilt or innocence hinged on this motive requirement at trial, did the district court err in refusing to give the *but-for* causation instruction requested by the defense?

**III. Multiple-count sentencing increase for single conviction of 18 U.S.C. § 2252.**

Under 18 U.S.C. § 2252(a)(4)(B), the "simultaneous possession of different matters containing offending images at a single time and place constitutes a single violation of the statute." *United States v. Chilaca*, 909 F.3d 289, 295 (9th Cir. 2018). Where a defendant was convicted of only one violation of 18 U.S.C. § 2252, but the district court imposed a "multiple count" adjustment that increased the advisory Sentencing Guidelines range to a high-end of 600 months' custody, did procedural error occur?

## Statement of Jurisdiction and Detention Status

Appellant [redacted] appeals his convictions for Attempted Sexual Exploitation of a Child, 18 U.S.C. § 2251(c) & (e), and Possession of Images of Minors Engaged in Sexually Explicit Conduct, 18 U.S.C. § 2252(a)(4)(B) & (b)(2).[1] The district court had jurisdiction under 18 U.S.C. § 3231. Following a jury trial and conviction, the court imposed sentence on February 26, 2020[2] and entered judgment on March 3, 2020.[3] [redacted] timely filed his notice of appeal on February 27, 2020,[4] and an amended notice of appeal on March 4, 2020.[5] This Court has jurisdiction under 28 U.S.C. § 1291.

[redacted] is in custody. His projected release date is October 10, 2038.[6]

---

1 Clerk's Record (hereafter "CR") at 1; Appellant's Excerpts of Record (hereafter "ER") at 104.
2 CR 238.
3 CR 247; ER 104.
4 CR 239; ER 112.
5 CR 248; ER 102.
6 *See* www.bop.gov (using inmate locator function).

## Statement of the Case

### I. The investigation, search and seizure, and arrest.

#### A. Overview: The F.B.I./Yahoo joint investigation.

In the summer of 2014, the U.S. Secret Service sponsored an "Electronic Crimes Task Force" conference.[7] It was attended by law-enforcement agents and their security counterparts at private corporations. The conference was designed so that "industry can . . . learn what the latest techniques are as far as underground crime or electronic crime."[8] At this government-sponsored event, Yahoo received a tip about potential child-exploitation activities on its platform. Although Yahoo reported this information to NCMEC[9], this case is really about its extraordinary coordination with federal law enforcement *beyond* that statutory framework—and beyond the reporting requirements for any child-pornography crime. Appellant [redacted] did not fall under suspicion for possessing or distributing child pornography on his online accounts. This is not a case about "hash values" or

---

7 ER 1753-1754.

8 ER 1754.

9 NCMEC is the National Center for Missing and Exploited Children. It was created by Congress, and per statute, receives all reports, or "Cybertips," of child pornography from internet service providers. Under 18 U.S.C. § 2258A, an internet service provider who learns about child pornography on their platform must make a report, called a "CyberTip" to NCMEC's "CyberTipline." *See* 18 U.S.C. § 2258A(a)(1)(B). *See also United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016) ("ISPs must report any known child pornography violations to NCMEC. Not to any other governmental agency, but again to NCMEC and NCMEC alone.").

other automated searches for known examples of digital contraband.[10] Indeed, [redacted] online accounts and communications were never shut down for violating terms and conditions of service, because they never contained any prohibited material.[11] Instead, [redacted] was targeted *because his internet service providers read his private communications outside of any lawful process, shared those communications and other private content extrajudicially with federal law enforcement, and did so—repeatedly—with the government's knowledge and acquiescence*.

This statement of facts (Section I) will first describe Yahoo's extraordinary campaign to build criminal cases for federal law enforcement—conduct that became "government action" under the Fourth Amendment. This campaign included:

- Secretly searching its customers' *private electronic communications*, and revealing them to the government without a warrant, subpoena, or even notice to the customer—all in violation of federal law;

- Organizing and leading *in-person briefings* with law-enforcement personnel to lay out their investigative findings, all outside of the NCMEC Cybertip process mandated by 18 U.S.C. § 2258A.

---

[10] "A hash value is (usually) a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm—and calculated in a way that makes it highly unlikely another set of data will produce the same value." *Ackerman*, 831 F.3d at 1294 (citing Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38-40 (2005)).

[11] *See* ER 1764. *See also* ER 1765.

- Providing reports "in a word doc" for law-enforcement agents "so you can copy-paste."
- Travelling with the F.B.I. to Manilla to help Filipino local police investigate crime;
- Offering behind-the-scenes technology to assist law-enforcement in developing probable cause;
- Drafting and giving joint presentations with the F.B.I. on their collective efforts and tactics;
- Recruiting other private entities to join the government and Yahoo in its "common goal" to fight child exploitation; and
- Avidly seeking updates and documentation of the arrests and convictions that these joint efforts garnered.[12]

Federal law enforcement then used Yahoo's information—and especially the private communications and personal data that it gathered warrantlessly—to obtain yet more private content from a different social media account managed by Facebook.

Finally, Section I will document how evidence resulting from these searches led to the warrants that were used to arrest and search [redacted] and his property, and to seize the evidence that was used to prosecute him. Together, the facts will demonstrate that this evidence was the fruit of repeated unlawful searches and seizures of [redacted] private online property, and that it amounted to "government action" under the law.

---

12 *See generally* ER 2060-2226.

### B. "Operation Swift Traveler" (2014-2016): Yahoo's unlawful searches of private communications, and its ongoing coordination with federal law enforcement, leads to the evidence against [redacted]

#### *1. Yahoo's "Electronic Crimes Investigation Team" and "Operation Swift Traveler."*

Yahoo is an internet service provider. Although it is a private company, it maintains a specialized department called its "Electronic Crimes Investigation Team." As the name suggests, its ECIT "investigates *criminal activity* [not merely compliance with terms and conditions] on Yahoo platforms."[13] ECIT is run by a former law-enforcement officer named Sean Zadig.[14] Zadig employs a host of other law-enforcement alumni in his unit,[15] and he maintains his network of relationships with former law-enforcement colleagues while working at Yahoo.[16]

The instant case began at an Electronic Crimes Task Force conference put on by the federal government.[17] At this conference, employees of Xoom.com (a money-transfer website) provided Yahoo with a tip about potential criminal activities involving pornography on its platform. Xoom later provided Yahoo with ten specific Cybertips,[18] alleging facts that Yahoo was then obligated to report to

---

13 ER 1720. *See also* ER 1750-1751.
14 ER 1749-1750.
15 ER 2042-2048.
16 ER 1751.
17 ER 1753.
18 *See* ER 2576.

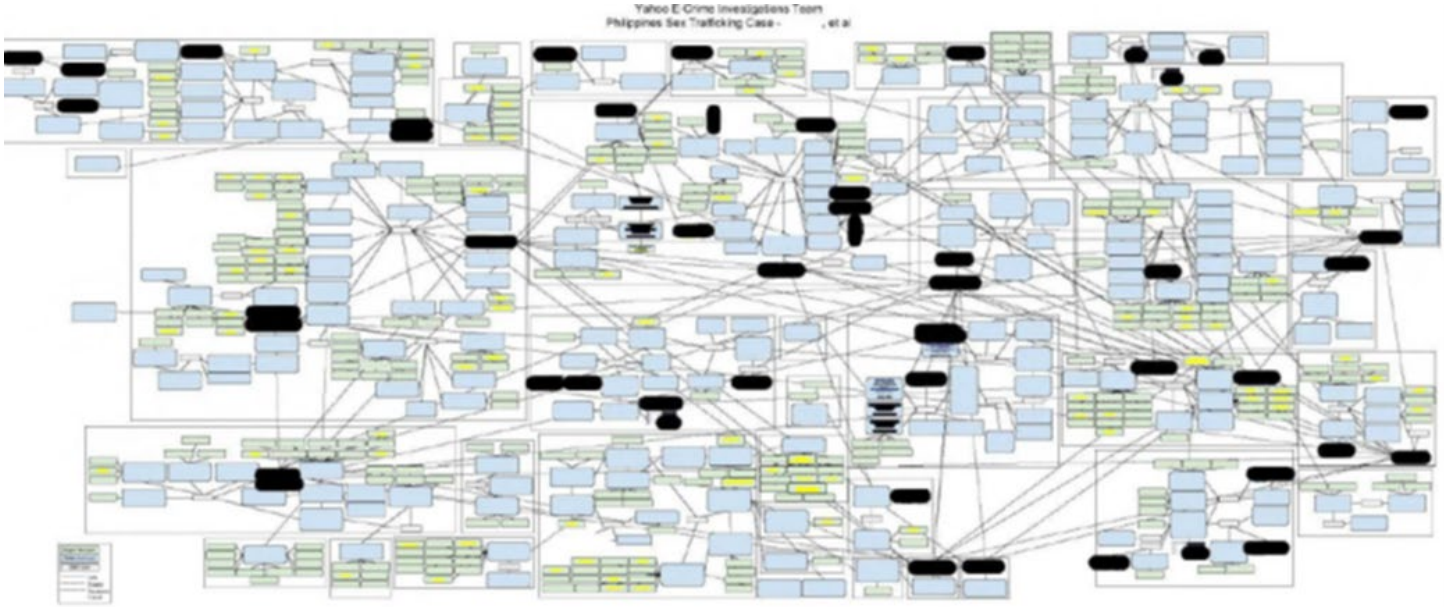
NCMEC.[19] Yahoo began an investigation into these accounts, and as required by law, reported its own findings to NCMEC.

But Yahoo's Electronic Crimes Investigative Team went much further. It built a sprawling criminal case for law enforcement to pursue. Its agent, Sean Zadig, flew to Alexandria, Virginia, to sit down with federal agents and discuss Yahoo's findings. These briefings became a regular occurrence: similar sit-downs ensued in October 2014, December 2014, and January 2016.[20] Zadig drafted a case chart depicting the investigation, entitling it the "Philippines Sex Trafficking

[19] *See, e.g.,* 18 U.S.C. § 2258(a)(1) (mandating reporting of known child pornography to NCMEC, upon threat of criminal sanction).

[20] *See, e.g.*, ER 1772-1773 (October 2014 meeting); ER 1952-1953 (December 2014 meeting); ER 1994 (December 2014 and January 2016 meetings).

Case." Here is the first such chart that Zadig unfurled on the conference room table:[21]



The chart depicts Yahoo's criminal suspects in blue and green. The lines represent either email communications or other links between suspects.[22] This information exceeded any reporting requirements or authorization set by statute.[23]

The F.B.I. responded by opening a formal investigation. It began submitting preservation requests to Yahoo,[24] issuing travel alerts, and subpoenaing financial

---

21 ER 2228.

22 *See* legend, *id.* at bottom left corner.

23 ER 1762 ("Q. [S]o this is something sort of above and beyond the statutory reporting requirements of federal law to the best of your knowledge anyway? A. Yes. To the best of my knowledge, the law just requires the CyberTip process to NCMEC. It doesn't go beyond that.").

24 *See* ER 2049-2059 (preservation requests to Yahoo in October 2014, December of 2014, March of 2015, and June of 2015).

records for these suspects.[25] Thus began one overarching investigation that spanned for the next several years—an investigation that eventually ensnared [redacted].[26]

### *2. The government knows that Yahoo is routinely searching and sharing private electronic communications—and does nothing to stop it.*

The Electronic Communications Privacy Act generally forbids internet service providers from sharing its users' private communications without a warrant or court order.[27] But Yahoo has been funneling its customers' private communications to the government for years, often outside the bounds of the mandatory-reporting scheme.[28]

---

25 *See generally* ER 2585-2589 (overview report of F.B.I. investigation).

26 *See, e.g.,* ER 1794-1795 (explaining how one set of reports built on the last); ER 1937 (describing overall Operation Swift Traveler); ER 1958 (F.B.I. knew that Yahoo was continuing to investigate); ER 1970-1971 (February of 2016, investigation still continuing and leading F.B.I. to Facebook materials).

27 *See, e.g.,* 18 U.S.C. § 2702 (prohibiting disclosure of electronic communications, even to law enforcement, subject to certain exceptions); 18 U.S.C. § 2703(b) (requiring either a warrant or specific notice to the consumer to obtain electronic communications); 18 U.S.C. § 3486 (same). Title 18 U.S.C. § 3486 (which governs administrative subpoenas generally) is in accord.

28 ER 1840 ("Q. Day in and day out for four years, Yahoo provided private Yahoo Messenger chats to NCMEC without it being requested by a warrant? [Objections overruled] . . . It wasn't unusual to do that? . . . [t]o provide Yahoo Messenger communications to NCMEC? A. [T]he messenger webcam investigations were unusual in that they were large scale and were not sort of our -- sort of day in and day out work on other platforms, *but this type of disclosure I would not consider unusual.*") (emphasis provided).

Many of the communications were taken from customers' "Yahoo Messenger" chats—conversations that Yahoo admitted were supposed to be "private communications between Yahoo customers."[29] From the beginning of this investigation, Yahoo repeatedly searched these private communications outside of any legal process, and shared them with the government.[30] Zadig conceded that these reports routinely included content which should have been protected by the Electronic Communications Privacy Act.[31] Indeed, these chats were not publicly visible, were sold to its customers as "private," [32] and were typically password-protected.[33] But unbeknownst to its customers, Yahoo intercepted the chat messages and read the "gist" of them.[34] It then provided the substance of those conversations to law enforcement.[35]

---

29 ER 1769 ("Q. And you would agree as a general manner, Yahoo Messenger chats are, in fact, private communications between Yahoo customers; true? A. [Zadig:] I would definitely agree with that. Q. And, in fact, it is described as such to Yahoo customers and in Yahoo literature; correct? A. That is correct.").

30 ER 1839-1841.

31 *See* 18 U.S.C. § 2702 (describing protected content and communications). *Cf.* ER 1736 (Zadig describing "information that is covered under ECPA, the Electronic Communications Privacy Act, within the initial referrals that we sent to NCMEC," and admitting that "the referrals . . . did provide some limited content or other information that might have been covered under that statute.").

32 ER 1769.

33 ER 1785-1786.

34 ER 1768.

35 ER 1768-1770. *See also* ER 1777 (Yahoo telling the FBI that it was reading "chat snippets" and "subject lines of e-mail accounts" of its customers to identify people who may be travelling to the Philippines).

Yahoo provided much of this content as so-called "supplements," directly to law-enforcement personnel, outside of the regular Cybertip process.[36] These reports included—for hundreds of customers in general, and for [redacted] in particular—the following information:

- The substance of private communications with other persons;[37]
- customers' personal information including full name, home address, and Facebook and Yahoo account details;[38]
- contact lists of who users communicated with;[39]
- phone numbers and email addresses;[40]
- "IP information" about the customers' internet addresses, including "metadata";
- background investigation gathered from sources outside of Yahoo, including sex-offender registries, military history, and travel history, "to help provide context around a particular user"[41] and,
- a proposed hierarchy of high-priority suspects.[42]

Zadig testified that these were motivated, at least in part, by federal mandatory reporting requirements.[43] But he also acknowledged that Yahoo's

---

36 ER 1726.

37 *Id.* *See also* ER 1768-1769 (describing monitoring chats to obtain the "gist of what was being communicated" and admitting that "sometimes" more had to be read because "the snippets that were visible were not enough").

38 *See* ER 2585-2587.

39 ER 1727.

40 *Id*.

41 ER 1728.

42 *See* ER 2399-2401.

43 ER 1725; *See also* ER 1809.

reports *exceeded* what was required by the relevant statutes.[44] In another criminal case arising from the same investigation, the district court judge asked Zadig what online conduct was "reportable" to NCMEC under the law. He answered as follows:

- He stated (accurately) that child pornography images and videos *must* be reported; [45]
- he acknowledged that Yahoo *chose to* disclose chat conversations or other text describing potential crimes, though he was vague about what authority permitted such a practice; [46] and,
- he asserted that mere conversations about obtaining child pornography, *without* any associated images, affirmatively *cannot* be reported to NCMEC.[47]

*The government had actual knowledge of these repeated private searches and extra-statutory disclosures, in the instant case, by October of 2014*.[48] F.B.I. Agent Yesensky, for example, admitted as much. He had worked full-time on the

---

44 ER 228-440.

45 ER 372-373. *Cf.* 18 U.S.C. § 2258.

46 *Id.* As discussed *infra*, this is not the law. Yahoo was only permitted to disclose content with a warrant or other court order, or in strict conformity with the exception set forth in § 2258.

47 *Id.* It remains unclear what authority Yahoo relies upon to distinguish these latter two reporting categories.

48 *See, e.g.,* ER 1776-1777 (admitting that Yahoo explained to the FBI that it was reading private chat snippets to discern travel habits as early as October 2014); *see also* ER 1782-1783: (Q: It is fair to say that you let law enforcement know that for at least these specific accounts, Yahoo was reading or obtaining the gist of their private Yahoo Messenger communications? [Zadig]: That's correct. Q: And they knew that as early as October 2014, federal law enforcement did? A: They did, correct.).

"Philippines Sex Case," aka "Operation Swift Traveler," from 2014 through at least 2017.[49] He served as a kind of "liaison" between federal law enforcement and other entities—and he considered Zadig a "key partner" in his endeavors.[50] He kept current on Yahoo's investigative tactics as part of his job.[51] More specifically, Yesensky testified that he knew "near the beginning" of the "broader overall Philippines Webcam Investigation" that Yahoo was reading and disclosing portions of password-protected communications.[52]

And the F.B.I. understood that Yahoo was continuing to conduct an *ongoing investigation* after the initial set of tips in October:

Q. . . . as we established earlier, Yahoo had submitted a number of these Philippines webcam related CyberTips October of 2014 or even earlier; right?

A. Correct.

Q. And then apparently between October of 2014 and your meeting in person in December of 2014, Yahoo had sent another batch of CyberTip reports, yes?

A. Correct.

Q. But those CyberTips were also related to the broader Philippines Webcam Investigation?

A. Yes.

Q. This ongoing investigation?

---

49 *See* ER 1686.
50 ER 2222.
51 ER 1980-1981.
52 ER 1949-1951.

A. Yes.[53]

. . . .

Q. So you understood, at least at some point after October, that Yahoo was continuing to do whatever they were doing on their end; right?

A. Yes, at some point after October, yeah.[54]

A year and a half later, in January of 2016, Yahoo was still providing similar reports, with similar contents, regarding the ongoing investigation—all with the F.B.I.'s full knowledge and acquiescence.[55]

### *3. [redacted] is discovered through Yahoo's ongoing chat searches—and the government has specific notice of the searches before they occur.*

This is exactly how the government built this case. Agent Yesensky acknowledged that these warrantless searches led directly to the evidence against [redacted].[56] Zadig confirmed the same.[57] Indeed, in 2015, Yahoo began collecting

---

53 ER 1952-1953.

54 ER 1957. Zadig also confirmed the ongoing nature of the investigation. *See* ER 1757-1758 ("Q: And the CyberTips, in your words, were related to an ongoing sex trafficking investigation; is that right? A. That's correct. "*The purpose of this e-mail was really to make sure that they understood that we were continuing to investigate,* and we had an initial set of CyberTips, and we wanted to not have those disseminated out to various places all over the world and treat it as one entity.").

55 ER 1974.

56 ER 1979 ("Q. And, in fact, chats regarding travel to the Philippines was some of the evidence that was ultimately gathered regarding [redacted] specifically; right? A. Yes.").

57 *See* ER 1737 (Zadig: "We believed on the chat snippets that we observed that [redacted] may have been a traveler, so somebody who was traveling to the Philippines, and we flagged the account as such in our referral.").

[redacted] *entire* chat history—not just snippets anymore—and warrantlessly provided private communications directly to federal law enforcement.[58] This evidence was all direct fruit of the initial searches that had occurred more than a year and a half earlier.[59]

The government knew about the searches before they happened. It did nothing to stop them. In July 2015, Zadig stated in an email, "*we're working on a new Philippines case. No idea how large it will be yet, we discovered it yesterday on some proactive scanning we're doing."*[60] And he promised that he "*will keep you informed. We do see some overlap with some of the buyers, but a different set of sellers. Lots of travelers again.*" Thus, almost a year after the first disclosures, the F.B.I. again had specific notice that Yahoo was doing "proactive scanning" of private online content, and that it would deliver the fruits of those warrantless searches to the government.[61] The F.B.I. happily went along with the process. The result was a January 2016 supplemental report that further incriminated [redacted][62]

---

58 ER 1739.
59 *See, e.g.,* ER 1794-1795, 1805-1806.
60 ER 2119 (emphasis provided).
61 *Id. See also* ER 1984-1985 (discussing email).
62 *See* ER 1876. The chats suggested an interest in travelling for purposes of illicit sex, but still contained no discussions of actual child pornography.

### *4. Arrests and convictions "are an outcome that we strive for": Yahoo's law-enforcement motives.*

Yahoo and Zadig specifically planned their actions to yield criminal arrests and convictions. Though Zadig claimed that Yahoo was enforcing its own terms and conditions, Yahoo *never shut down* [redacted] *account for violating its own rules*.[63] And Zadig acknowledged that the "common goal" of combatting child exploitation went beyond Yahoo's private business interests.[64] In fact, he recruited other entities for the express purpose of helping the F.B.I. with law-enforcement activities.[65]

He also conceded that the Electronic Crimes Investigative Team was, by definition, a crime-fighting unit within Yahoo whose work went beyond mandatory NCMEC reports. It provided "supplements" to the mandated NCMEC reports,

---

[63] ER 1764 ("Q. To the best of your knowledge, Yahoo never shut down [redacted] accounts for violation of Yahoo's terms and conditions; true? A. That's correct, yes. Q. And didn't shut down [redacted] accounts for violations of acceptable use policy; is that right? A. That is correct.").

[64] As discussed *infra*, a "common goal" with law enforcement is not an "independent" business purpose.

[65] *See* ER 1804-1805. ("*Q. The only purpose of making the introduction is to help IJM and the federal government combat child exploitation activity; right? A. Yes*. IJM has an expertise in the Philippines. They had a number of well publicized child rescues. They are also engaged in sort of rehabilitating children who have been abused, and I figured that that would be a relationship that would be very useful for the FBI. *Q. So the answer to my question was yes? A. Yes, that is correct*.") (emphasis provided).

including the charts and work product described above, that went above and beyond anything required by law.[66]

Zadig also volunteered tools and tactics to assist law enforcement in developing probable cause. Specifically, he offered digital third-party surveillance tools to help the government develop probable cause for warrants.[67] He even asked the FBI to obtain search warrants for other suspects on behalf of other, international law-enforcement agencies.[68]

Zadig maintained near-constant email contact with federal authorities.[69] And those emails revealed the extent of the joint investigation. For example, they show that Zadig:

- regularly corresponded with federal law enforcement throughout the investigation;[70]
- flagged suspects' travel plans based on their private messages;[71]

---

66 *See, e.g.,* ER 1725-1727.

67 ER 2103. *See also* ER 1790-1791. ("Q. Now, Mr. Zadig . . . you have no federal legal requirement to assist federal law enforcement in developing probable cause, do you? A. No, we do not. Q. *But, in fact, that is precisely why you were providing this tool is potentially to help them develop probable cause; right? A. So, yes.* Our concern was that the children who might be scantily clad in these profile pictures are still very likely being abused, and that was activity that we certainly wanted to see stopped. *Q. And the mechanism for getting that activity stopped is helping to provide probable cause to federal law enforcement; right? A. So in this e-mail, that is correct."*) (emphasis provided).

68 ER 1829.

69 *See generally* ER 2061-2226.

70 ER 2062.

71 ER 1835-1836.

- provided and received substantive updates;[72]
- coordinated the in-person meetings described above;[73]
- provided advance tips about reports that would be provided to NCMEC, and orchestrated follow-ups on the same;[74]
- advised NCMEC *not* to forward certain CyberTips to local or international law enforcement;[75]
- provided supplemental data above and beyond anything required by statute;[76]
- introduced third parties to the F.B.I. agent to further the "common goal";[77]
- and participated in a joint presentation in Manila along with the F.B.I., specifically to "help[] get the PNP [Philippines National Police] engaged in the webcam issue."[78]

Agent Yesensky corroborated these jointly undertaken actions. He confirmed Zadig's overall collaboration with law enforcement; that they spoke on the phone repeatedly; and that the FBI and Yahoo gave mutual updates on the investigation.[79] *He even testified that Zadig provided his reports in Word format, so that Yesensky could simply "copy-paste" text for legal process—including warrants.*[80]

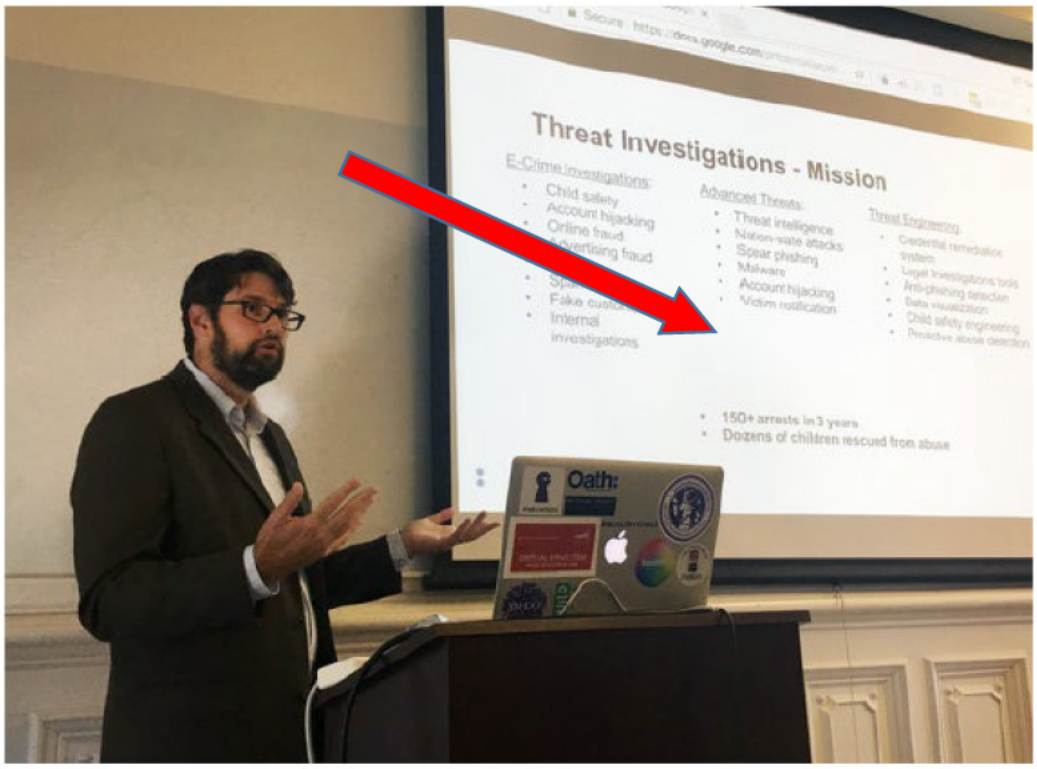
---

72 ER 2064, 2066, 2078.
73 ER 2092.
74 ER 2093.
75 ER 1828.
76 ER 2093-2094.
77 ER 2110, 2146.
78 ER 2117, 2119, 2133.
79 ER 1966-1967.
80 ER 1969-1970.

Yesensky also admitted that Zadig repeatedly requested information about whether his cases resulted in prosecution.[81] This included emails celebrating convictions against criminal defendants.[82] "Always appreciate the good news," Zadig wrote to Yesensky after reports of arrests;[83] to Zadig, the arrests were "a good reminder of why we do this work…."[84]

---

81 ER 1986.




Sean Zadig runs the threat investigations team at Oath, formerly known as Yahoo. He talked about his team's work at the Center for Long-Term Cybersecurity at the University of California, Berkeley in September.

*Alina Selyukh/NPR*

82 ER 1987-1988.

83 ER 2195.

84 *Id.*

Zadig admitted on the witness stand that arrests and prosecutions were, in his words, "one of the outcomes that we strive for."[85] These law-enforcement plaudits were a matter of personal pride for Zadig—to the extent that they literally became trophies on his wall.[86]


85 ER 1815. The photograph is from an NPR article included in the record at ER 2043-2046.

86 ER 2046.

Zadig acknowledged that arrests and convictions lent him "gravitas" in his field.[87] They also helped him "obtain support with the company for continued work and continued engineering improvements in this area."[88]

### C. 2017: Yahoo's searches lead law enforcement to search and seize private content from Facebook also.

[redacted] case was eventually parceled out from the national Operation Swift Traveler investigation to the San Diego field office. F.B.I. Agent Cashman became the local case agent. She acknowledged that she too reviewed the contents of [redacted] private chat communications, again warrantlessly.[89]

But by January of 2017, the investigation had gone cold. There was no information on open source media showing criminal activity.[90] Cashman had sent numerous emails to AUSAs trying to get a search warrant; the eventual response was that "the probable cause had become dated or stale."[91]

---

87 ER 1818.

88 ER 1823.

89 ER 1876. In the search warrant affidavit, Cashman claimed that the F.B.I. had obtained information through search warrants rather than Yahoo's extrajudicial disclosures, but she was later forced to admit that this was simply untrue. *See* ER 1908. Cashman had also originally claimed that other information had been provided by administrative subpoena, which was again proven to be factually false. *See* ER 1892 ("Q. As another example, the affidavit in Exhibit B indicates that there was identifying information related to [redacted] [redacted] that had been received pursuant to an administrative subpoena. Did you later determine that that was actually received as part of a NCMEC CyberTip rather than an administrative subpoena? A. I did later determine that, yes.").

90 ER 1907.

91 ER 1906.

But then Cashman received a Cybertip—a tip that Yahoo generated by reading [redacted] full chat communications. Receiving this tip belatedly, in late 2016 or early 2017, Cashman then sent a preservation request to *Facebook* in early 2017. Near the same time, she sent an email directly to NCMEC, asking that it too provide her with any information related to the [redacted] investigation.[92]

A Facebook employee explained the process that followed as a matter of course. Apparently, *every time* a law enforcement officer submits a subpoena or preservation request marked "child safety" or "exploitation," Facebook conducts an extrajudicial review of the account.[93] Though the review is initially limited temporally,[94] it includes "*messages*, timelines, photos, IP addresses, and machine cookies."[95] This occurs despite the fact that "messages are [supposed to be] private between Facebook users."[96] It requires no showing of cause or substantive evidence.[97] Literally every time an officer clicks "child safety" on Facebook's online subpoena portal, it automatically triggers warrantless review of the account.[98]

---

92 *See* ER 2606-2607.
93 ER 2011.
94 ER 2008.
95 ER 2013.
96 ER 2014.
97 ER 2010.
98 ER 2011-2013.

Federal mandatory-reporting requirements do the rest. If the bare allegation of "child safety"—and the warrantless review that always follows—shows anything of concern, Facebook conducts a deeper review, this time unfettered by time restraints.[99] If that review reveals any "child exploitation materials" on their platform, they "have an obligation to report it."[100] Facebook asserts that this policy has been in existence for years, and that it was exactly what happened in [redacted] case in 2017.[101] Agent Cashman acknowledged that her "preservation request did, in fact, result in Facebook providing to [her] through NCMEC content *that would otherwise require a warrant*,"[102] although she also claimed that it "was not my intended result."[103] Be that as it may, the warrantless searches yielded incriminating evidence that was then reported to NCMEC, which was promptly funneled back to Cashman. Cashman gathered up this evidence and included it in the search warrant affidavits.

---

99 ER 2013.
100 ER 2018. *See also* ER 2020 (discussing mandatory reporting to NCMEC).
101 ER 2020-2023.
102 ER 1903 (emphasis provided).
103 *Id*.

**D. The Resulting Search Warrant: Fruit of the Poisonous Tree and a Straw-man Affiant.**

Using the fruit of these searches, the F.B.I. requested search warrants for [redacted] property and home in June of 2017.[104] The warrants contemplated detailed searches of his digital devices. The affidavits were essentially identical for each warrant, and each identified four violations of law for which evidence was sought: 18 U.S.C. § 2251, § 2252, § 2252A, and § 2423.[105] The first three statutes relate to child pornography. Only the last one, § 2423, pertains to travel with the intent to engage in illicit sexual activity.

The supporting affidavit relied heavily—indeed almost exclusively—on the searches of [redacted] private communications described above. It described [redacted] communications with persons in the Philippines, where he appeared to be negotiating for sex with underage girls.[106] It described the other evidence that flowed from those original searches.[107] And then, it described the fruit of the Facebook and Yahoo searches that the government had instigated, as described above.[108]

---

104 *See* ER 2717-2774 (search warrant for person); ER 2776-2840 (search warrant of house).

105 ER 2717-2718.

106 *See* ER 2721-2728.

107 *See* ER 2728-2729.

108 ER 2729-2755.

It concluded that as a result, [redacted] "may" have collections of child pornography in his property and his home.[109]

But while the affidavit provided some evidence that [redacted] had discussed sex with underage girls in the Philippines, it did not establish probable cause for possessing or trafficking child pornography. Nevertheless, the affidavit contained the allegation, without evidence, that [redacted] "has also engaged in the production, distribution, and possession of images of minors engaged in sexually explicit conduct."[110]

But the images it referenced (suggestive but not lewd pictures of a girl who claimed to be 19 on Facebook) simply weren't child pornography—and the agent knew it. The agent failed to include the images themselves with the search warrant application. Nor did she describe the images. Tellingly, when Facebook reported these images to NCMEC, they did not classify them as child pornography either.[111] But the affiant did not disclose any of these facts. She chose to pretend that the images were child pornography, and to misleadingly describe the material as "child exploitation images"—whatever that means—instead.

---

109 ER 2758.

110 ER 2719.

111 *See* ER 2729, and Statement of Facts, *supra*, at II.E.

The evidentiary hearing confirmed that Cashman had never seen any images of child pornography related to the warrants.[112] Cashman testified that she based her claim in the affidavit on three things: 1) that [redacted] discussed erotic "selfies" with a person who held herself out as a 19-year-old on online chats, but who later turned out to be younger;[113] 2) [redacted] chatted with two other persons, expressing an interest in travelling to the Philippines to have sex with underage persons—but without ever discussing trading or viewing images of pornography;[114] and 3) her "training and experience."

Finally, though Cashman drafted the warrant, she did not swear it out. Rather, another agent testified that he was the search warrant affiant, despite the fact that he had almost literally no independent knowledge about the case or its facts.[115] He had never worked the case at all—even after learning that he would be the substitute affiant.[116] He had no independent knowledge of whether the

---

112 ER 1916-1917. In fact, as Sean Zadig testified, the previous three years of investigation by Yahoo and the F.B.I. resulted in *no* images of CP ever being found in any of [redacted] accounts. ER 1764-1765.

113 ER 1917. *See also* ER 1918 ("Q. So for and -- for the actual images that you saw chats about, being passed and back and forth, that had to do with a girl who said she was 19, then said she was 18, and the subscriber information said something different? A. Correct."). *See* ER 1920. And once they were viewed, they turned out to be nude pictures that never depicted any sexual activity. *Id.*

114 ER 1918-1919.

115 ER 1851, 1865-1866.

116 ER 1859-1860.

information in the affidavit had been obtained legally or illegally.[117] But none of this information was disclosed in the affidavit.

**E. Conclusion and Summary of Timeline.**

Thus, the following timeline is beyond dispute:

| Date: | Activity: | Citation: |
|---|---|---|
| July 2014 | Yahoo receives tip from Xoom at Secret Service hosted conference. | ER 1753-1754. |
| Oct. 2014 | Yahoo briefs federal law enforcement, in person, regarding "Philippines Sex Trafficking Case." | ER 1773-1775. |
| Oct. 2014 | Federal law enforcement learns that Yahoo is reading private "chat snippets" and email subject lines to reveal customers' travel habits. FBI accepts that content without warrant or court order. | ER 1777; ER 1782-1783; ER 1943; ER 1957. |
| Oct. 7, 2014 | FBI sends preservation letter freezing dozens of Yahoo accounts under 18 U.S.C. § 2703. | ER 2051. |
| Oct. 2014 | F.B.I. formally opens "Operation Swift Traveler" | ER 1939-1940. |
| Dec. 10, 2014 | Yahoo tells F.B.I. it has done even "more involved" searching and investigation, and schedules additional "in-person visit." | ER 2096. |
| Dec. 12, 2014 | Yahoo tells F.B.I. that "as before I will bring hard copies of the case report and case chart." | ER 2094. |
| Dec. 16, 2014 | Another in-person meeting between Yahoo and law enforcement; law enforcement again told that Yahoo is reading private communications to discern travel habits and personal information. | ER 1836; ER 2094 |

[117] ER 1867-1868.

| | | |
|---|---|---|
| Dec. 16, 2014 | Government first receives information about [redacted] and his activities in the Philippines from Yahoo. | ER 1737-1739; ER 1979, 2094. |
| Dec. 18, 2014 | Zadig provides supplemental report in a "word doc" to FBI Agent Yesensky "so you can copy-paste". | ER 2098. |
| Dec. 22, 2014 | Government sends preservation request freezing [redacted] Yahoo accounts under 18 U.S.C. § 2702(f). | ER 2052-2054. |
| Feb. 2015 | San Diego F.B.I. obtains lead regarding [redacted] from F.B.I. national-level Major Crimes Unit. | ER 1910. |
| March 17, 2015 | F.B.I. sends preservation request freezing [redacted] Yahoo account. | ER 2055-2056. |
| June 22, 2015 | Additional preservation letter freezing [redacted] Yahoo accounts; Yesensky and Zadig both on email thread. | ER 2057-2059. |
| July 23, 2015 | Zadig tells F.B.I. that he is working on more Philippines suspects, discovered during "some proactive scanning we're doing. Will keep you informed . . . . Lots of travelers again." | ER 2119.[118] |
| July 2015 | Yahoo searches [redacted] "full chat history on the Yahoo Messenger" and discloses contents to the government without a warrant or court order. | ER 1739. |
| Jan. 2016 | Yahoo provides Cybertip based on warrantless full chat history search that F.B.I. had notice about. | ER 1911. |

[118] In that same email, Zadig groused to F.B.I. Agent Yesensky that his legal department "nixed the travel to Europol, sorry [sad emoticon.] *They are a little wary of getting in front of an international [law enforcement] audience and talking about data disclosure and what my team does*. I don't really agree, but I have to do what they say. *I'm still good to go for Philippines, though*."). ER 2119.

| | | |
|---|---|---|
| Dec. 2016 | [redacted] investigation remains "stalled" out; San Diego F.B.I. unable to get search warrant application approved by U.S. Attorney's office, is told that the information had gone "stale." | ER 1906, 1911. |
| Jan. 2017 | San Diego F.B.I. receives additional Cybertip based on Yahoo's warrantless searching that had been submitted in 2016. | ER 1912. |
| Jan. 2017 | Prompted by new Cybertip (based on Yahoo searches of private communications) F.B.I. sends new preservation request to Facebook. | ER 1912. |
| Jan. 9, 2017 | FBI sends email to NCMEC again admitting that it has been receiving "chat" content warrantlessly, that the contents have to do with sex tourism, not child pornography, and that they have been unable to get a search warrant. | ER 2606-2607. |
| January 2017 | Upon receipt of preservation request marked "child exploitation," Facebook searches [redacted] accounts, reports contents to NCMEC, who funnels contents back to FBI agent. | ER 1903. |
| March 2017 | FBI sends additional preservation request to Facebook. | ER 2609-2613. |
| June 19, 2017 | Agent submits search warrant affidavit relying almost exclusively on private chats and contents revealed by Yahoo and Facebook warrantless searches. | ER 2717-2840. |
| June 21, 2017 | [redacted] arrested; property and home searched pursuant to warrant. | *See e.g.* ER 873-880.[119] |
| August 2019 | [redacted] convicted at trial based on evidence from June 2017 searches. | ER 448-449. |

[119] (These searches yield the first discovery of any material meeting the statutory definition of child pornography.)

## II. Proceedings and rulings in the district court.

[redacted] moved to suppress evidence, arguing that the initial Yahoo content, the subsequent Facebook content, the resulting search warrants, and the evidence seized pursuant to those warrants should all be suppressed under the Fourth Amendment.[120]

### A. Rulings on Fourth-Amendment Issues.

Specifically, [redacted] argued that the searches of his private digital content violated the Fourth Amendment; that the government's preservation orders and subpoenas were unlawful warrantless seizures under *United States v. Carpenter*;[121] and that the search warrant used to later seize his property were founded upon fruit of the poisonous tree and lacked probable cause anyway.[122] The district court denied each motion.[123]

#### *1. Searches and seizures of private correspondence on Yahoo.*

The district court first held that the government's use of information gathered by Yahoo did not violate the constitution, because it did not constitute "government action."[124] The district court further reasoned that "[t]he

---

120 *See, e.g.,* ER 2462-2508 (motion to suppress); ER 1680-1714 (renewed motion to suppress after evidentiary hearing).

121 138 S. Ct. 2206 (2018).

122 *See, e.g.*, ER 212-226, 1680-1714, 2462-2508.

123 *See, e.g.,* ER 11-16; ER 77-101.

124 *See* ER 89-90.

investigation of Yahoo ECIT pursuant to legitimate business purposes lead [sic] Yahoo to a duty to report under 18 U.S.C. § 2258A."[125] It concluded that "compliance with this duty to report did not convert Yahoo ECIT into a government actor subject to Fourth Amendment warrant requirements."[126]

The district court did not address the fact that the F.B.I. knew about the warrantless searches in advance of them occurring, nor did it address Zadig's stated intentions to obtain arrests and convictions.

***2. Preservation requests and subpoenas.***

[redacted] also argued that seizure of his records pursuant to preservation requests and subpoenas were unlawful under *Carpenter*. The district court denied that motion too,[127] holding *inter alia* that there was no legitimate expectation of privacy in the subpoenaed information under the third-party doctrine.[128] As to preservation requests to Facebook, it was undisputed that the subpoenas and requests, as a factual matter, led directly to Facebook searching [redacted] private communications—which could never have been done without a warrant—and that

125 *Id.*

126 ER 92.

127 ER 95. The preservation requests in this case were extended three different times, for a total of 270 days—far beyond the time period permitted by law. *See* ER 2050-2059.

128 ER 96.

once they did so, the government's reporting requirements mandated turning the fruit of these searches over to the government via NCMEC Cybertips.[129] But the district court held that this too was not a search.[130]

***3. Probable cause in Search Warrant.***

[redacted] next argued that while there may have been cause that he planned to engage in illicit sex in the Philippines, there was no probable cause to suggest that child pornography would be discovered in his luggage or at his San Diego home. The district court denied that motion also.[131]

**B. Conviction without but-for causation instruction.**

The case proceeded to trial. As part of his defense, [redacted] requested that the "purpose" *mens rea* required for conviction on Count 1 be defined for the jury. 18 U.S.C. § 2251(c) requires that an act be done "*for the purpose* of producing any visual depiction" of sexually explicit conduct involving a minor. Relying on *Burrage v. United States*, 571 U.S. 204 (2014), [redacted] requested an instruction requiring proof on Count 1 that "but for" an intent to produce a visual depiction, the sexual conduct would not have occurred. [132] The court rejected [redacted] request and instead instructed the jury that: "In order to prove the defendant acted

---

129 *See* Summary, *supra,* at I.E.
130 ER 97.
131 ER 98.
132 ER 1163-1168 and ER 1100-1110.

for purpose --for the purpose of producing a visual depiction of a minor engaged in sexually explicit conduct, the government must prove that the defendant's purpose was dominant, significant or motivating. The government is not required to prove that producing a visual depiction of a minor engaged in sexually explicit conduct was the sole purpose for defendant's conduct."[133]

[redacted] was convicted on both counts at trial.

### C. Errors at Sentencing.

Though the government only charged [redacted] with one count of possession of pornography in Count 3, it sought to punish him at sentencing for many different items within that count. [redacted] objected to the PSR using the Sentencing Guidelines' "multiple count" formulation for each of the images possessed in Count 3.[134] Though but one conviction of 18 U.S.C. § 2252 was returned in Count 3, the PSR calculated the Guidelines for what it called "Count 3A," "Count 3B," and "Count 3C."[135] The district court overruled [redacted] objections, and utilized this multiple-count methodology to increase [redacted] sentencing range up to high-end of 600 months' custody.[136]

---

133 ER 654.

134 ER 171-172 and ER 117.

135 Presentence Report ("PSR") at 12-14 (filed under seal).

136 *Id*. at 20. The court did not ultimately sentence within that range, but it was the "starting point" for the Guidelines analysis, and thus procedural error.

This appeal follows.

## Summary of the Argument

The conviction and sentence should be reversed for three reasons.

*First,* both counts of conviction relied on illegally obtained digital evidence. This evidence was the fruit of a years-long investigation, in which the government knowingly and repeatedly received private customer content that Yahoo disclosed unlawfully. Under virtually any of the recognized conceptions of "government action"—including the government's knowing acquiescence to Yahoo's violation of its customers' privacy, its complicity in a joint investigation with Yahoo and later Facebook, the exhaustive statutory scheme motivating and facilitating these extrajudicial searches, and Yahoo's stated intentions to use arrests and convictions as a tool to "clean up its platform"—these actions were subject to Fourth Amendment scrutiny. [redacted] motions to suppress should have been granted.

*Second,* [redacted] conviction on Count 1 should be reversed because the district court improperly instructed the jury on the "purpose" element required for Count 1. The Supreme Court has long taught that when a defendant's "purpose" is an element of a claim or defense, then that prohibited motive must be a "*but-for cause*" of the resulting act. *See, e.g., Gross v. FBL Fin. Servs.*, 557 U.S. 167, 180 (2009); *Burrage v. United States*, 134 S. Ct. 881, 888-90 (2014). Because the

district court refused that instruction here, error resulted, and the conviction should be reversed.

*Third*, under 18 U.S.C. § 2252(a)(4)(B), the "simultaneous possession of different matters containing offending [pornographic] images at a single time and place constitutes a single violation of the statute." *United States v. Chilaca*, 909 F.3d 289, 295 (9th Cir. 2018). [redacted] was convicted of only one violation of 18 U.S.C. § 2252 in Count 3, but the PSR recommended a "multiple-count" adjustment for "Count 3A" "Count 3B" and "Count 3C" based on different items of pornography. The district court accepted that analysis, increasing the applicable sentencing range to a high-end of 600 months' custody. That was procedural error, and a new sentencing should result even if the convictions are not reversed for the reasons stated above.

## Argument

### I. These convictions resulted from the unconstitutional search and seizure of private digital information.

#### A. Standards of review.

The legality of a warrantless search is reviewed *de novo*, see *United States v. Faagai*, 869 F.3d 1145, 1149 (9th Cir. 2017), as are warrantless seizures. *See United States v. Hernandez*, 313 F.3d 1206, 1208 (9th Cir. 2002). This Court reviews *de novo* whether a search constitutes "government action." *United States v.*

*Reed*, 15 F.3d 928, 930 (9th Cir. 1994). Whether a reasonable expectation of privacy exists is also reviewed *de novo*. *See United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). Factual findings regarding probable cause in a search warrant are reviewed for clear error, see *United States v. Hay*, 231 F.3d 630, 634 n.4 (9th Cir. 2000), but the review of search warrant's legality is *de novo*. *See United States v. Meek*, 366 F.3d 705, 712 (9th Cir. 2004).

### B. The Fourth Amendment applies to the government's repeated and knowing receipt of this evidence.

The Fourth Amendment protects against searches and seizures that are attributable to the government. *See United States v. Jacobsen*, 466 U.S. 109, 113–14 (1984); *United States v. Attson*, 900 F.2d 1427, 1429 (9th Cir. 1997). The record demonstrates 1) that a "search" and "seizure" of [redacted] private correspondence and data occurred; and 2) that these actions are attributable to the government here.

#### *1. The search: [redacted] digital content was constitutionally and statutorily protected.*

Modern Fourth Amendment jurisprudence recognizes that the government can violate either a reasonable expectation of privacy, *or* the security of one's papers, property, and effects. *See United States v. Jones*, 565 U.S. 400, 406 (2012). "[T]he *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test." *Lyall v. City of Los*

*Angeles*, 807 F.3d 1178, 1185 (9th Cir. 2015) (citation and punctuation omitted) (emphasis in original). Thus "the Fourth Amendment protects possessory and liberty interests even when privacy rights are not implicated." *Lavan v. City of L.A.,* 693 F.3d 1022, 1028-29 (9th Cir. 2012) (*citing Soldal v. Cook County,* 506 U.S. 506 56, 63-64 (1992)).

By obtaining [redacted] private online correspondence and other data without a warrant, the government and Yahoo[137] violated the Fourth Amendment under either paradigm.

*a. Digital "papers and effects."*

It is clear today that digital communications receive the same constitutional protections historically afforded to hardcopy "papers and effects." *See Grand Jury Subpoena v. Kitzhaber*, 828 F.3d 1083, 1090 (9th Cir. 2016) ("Personal email can, and often does, contain all the information once found in the 'papers and effects' mentioned explicitly in the Fourth Amendment."). In today's world, this content contains "the same kind of highly sensitive data one would have in 'papers' at home." *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013). Email, private "cloud" data, and text messages all fit into this category. *See United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (email); *Riley v. California*, 134 S.

[137] The extent to which this joint investigation constituted "government action" is considered *infra* at Section I.B.2.

Ct. 2473, 2491 (2014) (cell phones contents and cloud data); *Quon v. Arch Wireless Operating Co., Inc.*554 F.3d 769 (9th Cir. 2009), *rev'd on other grounds*, 560 U.S. 746 (2010) (text messages). Indeed, online platforms are "simultaneously offices and personal diaries," that "contain the most intimate details of our lives." *Cotterman*, 709 F.3d at 965. For many people today, one's "papers and effects" are *more* likely to be digital than hardcopy paper, and they deserve no lesser protection under the Fourth Amendment.

*b. A legitimate expectation of privacy exists in this private correspondence too.*

The searches violated a reasonable expectation of privacy also. There is a well-established privacy interest in sealed mail, see *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (citing cases), and the law is clear that "email should be treated like physical mail for purposes of determining whether an individual has a reasonable expectation of privacy in its content." *Grand Jury Subpoena v. Kitzhaber*, 828 F.3d 1083, 1090 (9th Cir. 2016). *See also Forrester*, 512 F.3d at 511 (same).

Text messages are no different. The Court held in *Quon v. Arch Wireless Operating Co., Inc.*, that "[w]e see no meaningful difference between the e-mails at issue in *Forrester* and the text messages at issue here." 529 F.3d 892, 905 (9th Cir. 2009), *rev'd on other grounds,* 560 U.S. 746 (2010). The expectation of privacy remains, even vis-à-vis service providers who host or facilitate the

correspondence. *Id.* ("That [the service provider] may have been able to access the contents of the messages for its own purposes is irrelevant."). For this same reason, the Supreme Court has observed that "text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." *City of Ontario, Cal. v. Quon*, 560 U.S. 746, 760 (2010).

This case involves private "Yahoo Messenger" communications and private Facebook messages. Both fall squarely into the case law described above. *See also R.S. ex rel. S.S. v. Minnewaska Area School Dist.*, No. 2149, 894 F.Supp.2d 1128, 1142 (D. Minn. 2012) (finding "a reasonable expectation of privacy [in] private Facebook information and messages"). Both Yahoo Messenger and "private Facebook messages are, like email, inherently private," and as such "are not readily accessible to the general public." *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965, 991 (C.D. Cal. 2010). Both are thus constitutionally protected. Yet both were searched by online service providers outside of any legal process or notice to the consumer, and simply handed over to federal law enforcement. In Yahoo's case, they were searched warrantlessly and turned over directly to the F.B.I. in sit-down meetings in Alexandria, Virginia, and included in "supplemental reports" that occurred outside of any warrant—or even administrative—process. For Facebook, they were also searched warrantlessly as the result of a preservation

request, and funneled through NCMEC into the waiting arms of the F.B.I. On both counts, this was an intrusion into both [redacted] "papers and effects" and a violation of his legitimate expectations of privacy.

And not only is society "prepared to recognize" that these communications are private under *Katz's* formulation—in reality, society already does. *See* Christine S. Scott-Hayward, Henry F. Fradella & Ryan G. Fisher, *Does Privacy Require Secrecy? Societal Expectation of Privacy in the Digital Age*, 43 Am. J. Crim. L. 19, 55 (Fall 2015).[138] Indeed, even two of the largest corporate internet service providers in the world—Google and Facebook—recently filed a joint amicus brief with this Court, agreeing that its customers enjoy a reasonable expectation of privacy in their online communications. *See United States v. Luke Wilson*, 18-50440, Brief For Amici Curiae Google LLC and Facebook, Inc., at 18. According to Google and Facebook, this is so *even if users violate a company's Terms of Service*. As *amici* argued:

> *A user's reasonable expectation of privacy in email is not defeated by a provider's ability to access its content or by a service provider's Terms of Service* for the reasons explained in the Brief of Amici Curiae Electronic Frontier Foundation & American Civil Liberties Union Foundation. See EFF & ACLU Br. 10-12. *Rather, the Fourth Amendment generally protects*

[138] According to the article, "Over 90%" of respondents report they 'felt that law enforcement should never have access, or at least require a level commensurate with probable cause, to obtain access to text, multimedia, or voicemail messages on cell phone." *Id.*

> *users' reasonable expectations of privacy in the contents of emails held by a third-party service provider from warrantless search and seizure by the government, irrespective of whether the service provider has terminated that user's account or whether the user violated the terms governing his relationship with the service provider*. *United States v. Mohamud*, 843 F.3d 420, 442 (9th Cir. 2016), cert. denied, 138 S. Ct. 636 (2018); *see also Byrd v. United States*, 138 S. Ct. 1518, 1524 (2018) (drivers have a reasonable expectation of privacy in a rental car even when driving the car in violation of the rental agreement); *United States v. Warshak*, 631 F.3d 266, 286-88 (6th Cir. 2010).
>
> *Id.* at 18.

Here, there is no evidence in the record that [redacted] agreed to any particular terms and conditions, or violated the same, so that is not an argument that can be considered anyway. *See United States v. Davis*, 785 F.3d 498, 510 (11th Cir. 2015).[139] But it is telling that even massive internet service providers like Google and Facebook have filed briefs urging this Court to recognize a privacy interest in online communication even when it may violate those policies.

Ultimately, "a person does not forfeit his expectation of privacy merely because [the data] is located in a place that is not controlled exclusively by the container's owner." *Kitzhaber*, 828 F.3d at 1090 (citing *United States v. Monghur*, 588 F.3d 975, 978 (9th Cir. 2009) (citation omitted). For all of these reasons,

---

[139] *Id.* ("Although [the defendant] would have signed a contract when beginning service with [that ISP] *that contract does not appear on this record to have been entered into evidence here*. *Thus we cannot consider it, or [that] privacy policy, in this particular case*.") (emphasis provided).

[redacted] had a reasonable expectation of privacy in his private online communications and a right to the integrity of his "papers and effects."

*c. The monitoring and disclosure of this private correspondence also violated federal statute.*

These privacy rights are further underscored by federal statute as it existed at the time of the searches. The Electronic Communications Privacy Act forbids disclosure of private communications (like emails and text messages) to third parties, subject only to tightly drawn exceptions. 18 U.S.C. § 2702(a)(1) provides that "a person or entity providing an electronic communication service to the public [like Yahoo or Facebook] shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." Even the government cannot obtain these communications without a warrant. *Id.* at § 2703.

These statutes are not a regulatory technicality. Rather, they protect a traditional "*substantive* right to privacy," the violation of which is a "concrete harm" to the communications' owners. *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1117 (9th Cir. 2020) (emphasis in original). In *Campbell*, this Court "conclude[d] that the statutory provisions . . . protect concrete interests because . . . they 'codif[y] a context-specific extension of the *substantive* right to privacy.'" *Id.* (emphasis in original) (quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017)). Indeed, *Campbell* held that when an internet service provider

"identifies and collects the contents of users' individual private messages"—exactly what Yahoo did here—that represents "a violation of the concrete privacy interests" protected by law.

And mandatory-reporting requirements did not justify the violation, nor provide an exception to the constitutional or statutory rules. As a threshold matter, a federal statute cannot override Fourth Amendment protections. If federal mandatory-reporting requirements stretch beyond what the Fourth Amendment permits, then they are facially unconstitutional. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) ("because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of [defendant's] emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.").[140]

But federal statute did not justify these disclosures in any event. The exception to the ECPA's privacy requirements is found in the mandatory-reporting requirements of 18 U.S.C. § 2258A. That statute permits Cybertips to NCMEC when—and only when—an electronic service provider acquires knowledge of

---

[140] *See also City of L.A. v. Patel*, 576 U.S. 409, 417 (2015) (finding municipal statute requiring hotel operators to open books to police facially unconstitutional). *See also Ferguson v. Charleston*, 532 U. S. 67, 86 (2001) (holding that a hospital policy authorizing "nonconsensual, warrantless, and suspicionless searches" contravened the Fourth Amendment).

apparent *child pornography offenses*. Specifically, reportable circumstances under § 2258A are "facts or circumstances from which there is an apparent violation of [18 U.S.C. ] § 2251, 2251A, 2252, 2252A, 2252B, *that involves child pornography*; or section 1466A."[141] Every one of these statutes govern actual child pornography; none deal with travel for illicit sexual conduct.

Notably, alleged travelling for purposes of illicit sexual conduct under 18 U.S.C. § 2423 is not included on the list of reportable offenses. When a report *is* authorized, it is permitted to include: information about the individual; historical information about the discovery of child pornography; geographic location information; the images of child pornography themselves; and the "complete communication containing any image of apparent child pornography." 18 U.S.C. § 2258A(b)(1)-(5). Nothing in § 2258A permits disclosure of private communications for other purposes, including alleged travel for illicit sex. By reading and disclosing emails that related to travel for sexual purposes but did not involve child pornography, Yahoo acted beyond the statutory framework of § 2702

---

[141] In 2018, Congress amended § 2258A to permit reporting when "facts or circumstances . . . indicate a violation of any of the sections described in subparagraph (A) involving child pornography may be planned or imminent." But that language did not exist at the time of [redacted] reports. Moreover, neither the government nor Yahoo has relied upon that language to justify these extrajudicial disclosures, and it does not fit the facts here even if they did.

and § 2258A. These were illegal searches that violated the constitution and federal statute, and were not saved by any mandatory-reporting requirements.

### *2. Government action: the searches were constitutionally attributable to the government.*

Once a "search" occurs, the question becomes whether that search should be attributed to the government for Fourth Amendment purposes. The answer here is yes.

#### *a. As an initial matter, all of NCMEC's actions are government action.*

Preliminarily, this Court should confirm that NCMEC is itself a government actor in this context. Case law demonstrates that not only does NCMEC work closely with the government, but that for Fourth Amendment purposes, it *is* the government. Then-Circuit Judge Gorsuch addressed this issue in *United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016). *Ackerman* squarely held that NCMEC was a governmental actor. *Id.* at 1295. This holding rested upon:

- NCMEC's law-enforcement functions, which have traditionally been reserved for police. *Id.* at 1295-96.
- NCMEC's two authorizing statutes—18 U.S.C. § 2258A and 42 U.S.C. §5773(b)—which mandate its collaboration with law enforcement "in over a dozen ways." *Id.* at 1296.
- That service providers must report known child pornography to NCMEC or face criminal penalties. *Id.* (citing 18 U.S.C. § 2258(a)(1)).

- Service providers must treat a NCMEC report as a request to preserve evidence issued by the government itself—again under threat of criminal sanction. *Id.* at 1297 (citing 18 U.S.C. § 2258A(h)(1), § 2703(f)(1), § 2258B).
- NCMEC alone is allowed to knowingly possess and review child pornography pursuant to its statutory functions. *Id.* And,
- The vast "day to day statutory control" and budgetary power that the federal government exercises over NCMEC. *Id.* at 1298.

*Ackerman* also reasoned that even if NCMEC wasn't actually a government entity, that it was a government *agent* for Fourth Amendment purposes. *Id.* at 1300-1303. It pointed to the government's knowledge and acquiescence in NCMEC's searches; the fact that it "encouraged and endorsed and participated" in NCMEC's searches; and NCMEC's purpose in aiding law-enforcement to reach that conclusion. *Id.* Even a cursory review of cases in this Circuit supports *Ackerman*'s conclusion, as NCMEC and law enforcement unquestionably work hand-in-glove.[142]

*Ackerman*'s logic is unassailable, and should be adopted here. Thus, every time Yahoo gave NCMEC a tip, it was giving it to the government. The same is true of Facebook's interactions with NCMEC. And when NCMEC gathered and exchanged information with both companies and the F.B.I., it was legally no

---

142 *See, e.g., United States v. Kennedy*, 643 F.3d 1251, 1255 n.8 (9th Cir. 2011) (describing NCMEC's role in criminal investigation); *United States v. Daniels*, 541 F.3d 915, 920 (9th Cir. 2008) (same).

different than the F.B.I. doing so directly, at least for Fourth Amendment purposes. In sum, if NCMEC was instigating, encouraging, or facilitating a search, it was *the government* instigating, encouraging or facilitating the search. Funneling searches and seizures through NCMEC does not alter the Fourth Amendment issues at stake here.

*b. Yahoo's searches amounted to "government action" because law enforcement acquiesced to the illegal acts, they were intended to further criminal prosecutions, and because they were part of overarching federal legislation encouraging warrantless searches.*

Yahoo's repeated searches were "government action" too. While some of this Court's opinions suggest that this issue is assessed through a rigid two-pronged test, *see, e.g.*, *United States v. Cleaveland*, 38 F.3d 1092 (9th Cir. 1995), that conflicts with Supreme Court precedent describing a totality-of-the-circumstances approach. *Skinner v. Ry. Labor Executives' Ass'n,* 489 U.S. 602 (1989) said so unmistakably: "Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities," the Court observed, which is "*a question that can only be resolved 'in light of all the circumstances.'*" *Id.* at 614 (emphasis provided).[143]

[143] *See also Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971) ("The test . . . is whether [the private party] *in light of all the circumstances of the case*, must be

Here, the district court expressed the "government action" test more restrictively, as: "(1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends." ER 89 (citing *United States v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982)). But it is unnecessary to decide whether the *Miller* test unfairly restricts the totality-of-the-circumstances standard. The record here demonstrates government action either way.

i. Government knowledge and acquiescence.

First, this Court's precedent recognizes "the maxim that 'if the state knowingly accepts the benefits derived from unconstitutional behavior then the conduct can be treated as state action.'" *Tsao v. Desert Palace, Inc.*, 698 F.3d 1128, 1140 (9th Cir. 2012) (quoting *Nat'l Collegiate Athletic Ass'n v. Tarkanian*, 488 U.S. 179, 192 (1988) (internal punctuation omitted)). *See also Gorenc v. Salt River Project Agric. Improv. & Power Dist.*, 869 F.2d 503, 507 (9th Cir. 1989) same).[144] Indeed, advance government knowledge *alone* can invoke the Fourth

---

regarded as having acted as an 'instrument' or agent of the state."). As this Court itself has acknowledged, "the Fourth Amendment applies to a search whenever the government participates *in any significant way* in this *total course of conduct.*" *United States v. Davis*, 482 F.2d 893, 896-97 (9th Cir. 1973) (emphasis provided; internal citations and punctuation omitted).

[144] While *Tsao* and *Gorenc* analyzed this rule in the context of lawsuits brought under 42 U.S.C. § 1983, it should be no different in a criminal case. If anything, the Fourth Amendment should protect a criminal defendant *at least* as much as it does a civil plaintiff.

Amendment's protections. *See United States v. Jacobsen,* 466 U.S. 109, 113-14 (1984) ("This Court has also consistently construed [the Fourth Amendment's warrant requirement] as proscribing only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government *or with the participation or knowledge of any governmental official*'") (quoting *Walter v. United States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)).

And when the government repeatedly accepts the fruit of warrantless private searches, it becomes government action—even when it did not know that a *particular* private search was forthcoming. In *United States v. Walther*, 652 F.2d 788 (9th Cir. 1981), for example, a private airline employee opened a passenger's package and discovered drugs. He turned the drugs over to the DEA. Although this single act, standing alone, might have been a private search, it "was not [the private employee's] first contact with the DEA." *Id.* at 790. The private party had performed searches multiple times before, even receiving payments on some of them. *Id.* The private party continued to perform additional searches for drugs after the payments from the DEA stopped as well. This Court held that the pattern of prior searches "provides proof of the government's acquiescence in the search." *Id.* at 793. "While the DEA had no prior knowledge that this particular search would be conducted and had not directly encouraged [the employee] to search this

overnight case," the DEA knew that "had opened [luggage] before, and did so with no discouragement from the DEA." *Id.* "The DEA thus had knowledge of a particular pattern of search activity dealing with a specific category of cargo, and had acquiesced in such activity." *Id.*

Similarly, in *United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994), a hotel manager opened closed drawers in a guest room and opened a latched briefcase while police officers stood in the doorway watching. Though they did not actively participate in the search, this Court held that the officers' knowing acquiescence to the search amounted to government action, and that the Fourth Amendment applied. *Id.* at 932. As this Court held in *United States v. Davis*, "even if governmental involvement at some point in the period could be characterized accurately as mere 'encouragement,' or as 'peripheral' . . . that involvement would nevertheless be 'significant' for purposes of the Fourth Amendment. Constitutional limitations on governmental action would be severely undercut if the government were allowed to actively encourage conduct by 'private' persons or entities that is prohibited to the government itself." 482 F.2d 893, 904 (9th Cir. 1973).

*Here, the government had actual knowledge of these repeated private searches and extra-statutory disclosures by October 2014.*[145] The F.B.I. agent testified that he knew "near the beginning" of the "broader overall Philippines Webcam Investigation" that Yahoo was reading and disclosing portions of password-protected communications.[146] Thus, even if the government did not specifically ask Yahoo to search [redacted] accounts in 2014, they acquiesced to repeated searches of private communications that they had known about since at least the prior October, and they knew that more of the same searches were occurring that December. That is more than sufficient to establish government action under *Tsao*, *Gorenc*, *Walther* and *Reed.*

And later, in advance of *another* meeting in 2016, the F.B.I. received even more specific notice of ongoing searching—this time including the prospect of "proactive scanning,"[147] and notice of Yahoo customers' travel plans.[148] It met

---

145 *See, e.g.*, ER 1776-1777 (admitting that Yahoo explained to the FBI that it was reading private chat snippets to discern travel habits as early as October 2014); *see also* ER 1782-1783: ("Q: It is fair to say that you let law enforcement know that for at least these specific accounts, Yahoo was reading or obtaining the gist of their private Yahoo Messenger communications? [Zadig]: That's correct. Q: And they knew that as early as October 2014, federal law enforcement did? A: They did, correct.").

146 ER 1948-1950.

147 ER 2119 (July 2015 email regarding "proactive scanning").

148 ER 2158 ("You may want to take a look at CyberTip 7931273. Individual planning to travel in February.")

again with Yahoo, in person, to receive the fruits of the searches.[149] Because the "police cannot acquiesce to or indirectly encourage a private person's search for incriminating evidence without implicating the Fourth Amendment," *Reed*, 15 F.3d at 933, that was government action.

The same is true of Facebook's searches. The evidence shows that, unbeknownst to customers, *every time* Facebook gets a preservation request labeled as a "child-exploitation" or a "child safety" matter, it conducts a warrantless search.[150] And while agent Cashman claims that *she* had no idea that such a search would result, this was certainly not the first administrative subpoena that an FBI agent sent to Facebook. "Where law enforcement authorities are cooperating in an investigation, the knowledge of one is presumed shared by all." *United States v. Jensen*, 425 F.3d 698, 704 (9th Cir. 2005) (quoting *Illinois v. Andreas*, 463 U.S. 765, 772 n.5 (1983)). The F.B.I., as an entity, knew that marking subpoenas "child exploitation" resulted in Facebook carrying out warrantless searches. The first *Miller* prong—knowledge and acquiescence of both warrantless searches—is met here.

---

149 *See, e.g.,* ER 2157 (setting up meeting for "latest webcam case" in January 5, 2016 email).

150 ER 2007-2013.

ii) Purpose of assisting law enforcement.

The second *Miller* prong is met too. If a private party acted with the intent to assist the government in enforcing the law, it is also government action. Put differently, an otherwise-private search must comply with the Fourth Amendment if "its purpose [is] to elicit a benefit for the government in either its investigative or administrative capacities." *See United States v. Reed*, 15 F.3d 928, 931-32 (9th Cir. 1994) (private security officer's search of hotel room was government action because it was "intended to assist the police" and "a private carrier's interest in preventing criminal activity was not a legitimate independent motivation.")[151]

The district court's ruling boils down to the claim that Yahoo and Facebook were really acting with private motives in carrying out these warrantless searches. But setting aside that this claim is undermined by the facts,[152] this also

---

[151] Even mixed motives create government action if one of them evinces a law-enforcement purpose. *See Mann v. Cty. of San Diego*, 907 F.3d 1154, 1161-62 (9th Cir. 2018) (where law-enforcement and non-law-enforcement purposes both exist simultaneously, it is government action). *See also Greene v. Camreta*, 588 F.3d 1011, 1026-27, 1029 (9th Cir. 2009), *vacated in part as moot* 661 F.3d 1201 (9th Cir. 2011); *Roe v. Texas Dep't of Protective & Regulatory Servs.*, 299 F.3d 395, 406-07 (5th Cir. 2002) (holding that social workers' investigations regarding alleged child abuse are not "divorced from the State's general interest in law enforcement" because they function "as a tool both for gathering evidence for criminal convictions and for protecting the welfare of the child").

[152] To this day, Yahoo has not suspended [redacted] account for any purported violations of its terms and conditions. And despite an 18-month investigation, no child pornography was ever discovered. The evidence shows a clear purpose of investigating crime and turning the evidence over to law enforcement instead.

misconstrues the law. Legally, preventing child-exploitation crimes is a law-enforcement motive. While it is admirable and understandable, crime prevention is simply not an independent motive that will excuse Fourth-Amendment inquiry. *United States v. Walther*, 652 F.2d 788, 792 (9th Cir. 1981), squarely held that a private carrier's interest in preventing criminal activity was not a legitimate independent motivation. Indeed, "if crime prevention could be an independent private motive, searches by private parties would never trigger Fourth Amendment protection and the second prong of the *Miller* test would be meaningless." *Id.* *See also United States v. Reed*, 15 F.3d 928, 932 (9th Cir. 1994) (holding that hotel management's desire to keep hotel free of criminal activity is not an independent motive, but rather crime prevention and thus government action). This is particularly true here, where both Yahoo and Facebook also assert that they were conducting internal searches in an effort to comply with the law governing mandatory-reporting requirements.

But even if the *ultimate goal* was related to private business, getting arrests and convictions was the means to that goal—and thus provided an *immediate objective* sufficient to trigger Fourth Amendment protections. *Ferguson v. City of Charleston*, 532 U.S. 67, 82-8 (2001), helps explain the distinction between these "ultimate goals" and the "immediate objective" utilized to achieve those ends. There, a hospital drug-tested pregnant women and referred mothers who tested

positive to law enforcement. The Supreme Court rejected the argument that the search was not for a law-enforcement purpose, and held that the hospital's "immediate"—as opposed to "ultimate"—goal is what counts under the Fourth Amendment. "While the ultimate goal of the program may well have been to get the women in question into substance abuse treatment and off of drugs," the Court reasoned, "*the immediate objective of the searches was to generate evidence for law enforcement purposes in order to reach that goal*." *Id.* at 82-83. "The threat of law enforcement may ultimately have been intended as a means to an end, but the direct and primary purpose of MUSC's policy was to ensure the use of those means. In our opinion, this distinction is critical." *Id.* at 83-84.

Here, Zadig acknowledged that arrests and prosecutions were a means of "deterrence" and helped to "push this content to other platforms." Under *Ferguson*, that suffices to show motive.

Ultimately, even if there were independent motives, "the mere existence of a legitimate independent motive apart from crime detection or prevention does not immunize a search from scrutiny regardless of the level of government involvement." *Cleaveland*, 38 F.3d at 1094. For all of these reasons, Yahoo's "intent" under the *Miller* prong supports a finding of government action too.

iii) The searches were government action insofar as they were encouraged by federal statute and overarching government initative.

A company's response to statutory regulation and/or an overarching government initiative cannot be a legitimate independent business purpose either. In *Skinner v. Ry. Labor Executives' Ass'n* 489 U.S. 602 (1989), the Court held that government regulations that encouraged railroads to drug-test its employees implicated the Fourth Amendment. Where the government removed legal barriers to drug testing, "made plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions," and "mandated that the railroads not bargain away the authority to perform tests" the Court held that "[t]hese are clear indices of the Government's encouragement, endorsement, and participation, and suffice to implicate the Fourth Amendment." 489 U.S. at 615-16. Importantly, the statute at issue in *Skinner*, "Subpart D" of the statutory scheme, did not *require* the searches; rather, it merely permitted them. *Id.* at 611.[153] The Supreme Court nevertheless held that *optional* private searches, carried out in reliance on authorizing federal statute, was tantamount to government action.

[153] ("Subpart D of the regulations . . . is *permissive. It authorizes* railroads to require covered employees to submit to breath or urine tests in certain circumstances not addressed by Subpart C.") (emphasis provided).

There is a similar statutory framework in place here. 18 U.S.C. § 2701 *et seq*., the Stored Communications Act, reflects the general principle that a person's online communications are private, and ought not be shared with third parties. Indeed, § 2701(a) and (b) criminalize intentionally *accessing* electronic communications under most circumstances. But § 2701(c)(1) and (c)(3) arguably carve out an exception for internet service providers like Yahoo to do just that, clearing the way for service providers to monitor customer communications that would otherwise be private. Likewise, while § 2702 prohibits the *disclosure* of customer communications, § 2702(b)(6) creates an exception for reports to NCMEC (as occurred in [redacted] case) pursuant to 18 U.S.C. § 2258A. And § 2258A *mandates* reports to NCMEC when service providers come across apparent child pornography. Taken together then, the Stored Communications Act allows internet service providers to access and read private communications that are otherwise constitutionally protected "papers and effects." It then *requires* the provider to share that information with law enforcement (via NCMEC) if it is something that the government has deemed contraband. That creates the kind of feedback loop that ensnared [redacted] in this case—and that works around the warrant requirement otherwise required for searches and seizures. Simply put, if a federal statute allows companies to read and disclose private papers and communications, and the government to receive them without a warrant, then it

violates the constitution and cannot be a legitimate business purpose. *See United States v. Warshak,* 631 F.3d 266, 288 (6th Cir. 2010) ("to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.").[154]

The government may argue § 2701 *et seq.* does not *mandate* affirmative searching, but merely *permitted* it. But that is a search under *Skinner* too. While cases interpreting *Skinner* often focus on the mandatory-searching portion of that case and statutory scheme, that was not the only kind of regulation at issue. *Skinner* also involved a *permissive* searching scheme, and addressed whether that amounted to government action.[155] There, the Supreme Court squarely held that even searches permitted (but not mandated) by federal statute were government action. *Id.* at 615-16.

So it is here. Subsection (c) of § 2701 allows internet service providers to access communications that are constitutionally private, and otherwise protected

---

[154] *See also City of L.A. v. Patel*, 576 U.S. 409, 417 (2015) (finding municipal statute requiring hotel operators to open books to police facially unconstitutional). *See also Ferguson v. Charleston*, 532 U. S. 67, 86 (2001) (holding that a hospital policy authorizing "nonconsensual, warrantless, and suspicionless searches" contravened the Fourth Amendment).

[155] *See id.* at 606 (the Railroad Administration "*also has adopted regulations that do not require, but do authorize* railroads to administer breath and urine tests to employees who violate certain safety rules. *The question presented by this case is whether these regulations violate the Fourth Amendment*."). *See id.* at 611 ("The relevant portion here is "Subpart D of the regulations, which . . . *is permissive*.")*.*

by statute. It arguably allows third parties to access these same communications too—a glaring exception to traditional expectations of privacy and security in one's papers. And 18 U.S.C. § 2258A trumps the Electronic Communications Privacy Act in this context too, permitting disclosures that would otherwise be forbidden and providing a statutory safe-harbor for these otherwise-unlawful reports. And it is uniquely mandatory. Parcel carriers and hardcopy booksellers, for example, do not seem to have the same duties to report. But internet service providers face criminal penalties if they don't report contraband to NCMEC; NCMEC reports are automatically reported to law enforcement; and a Cybertip is simultaneously a preservation request back to the service provider. *See generally* 18 U.S.C. §§ 2702, 2258A. And even where a service provider is not required to affirmatively seek out child pornography, the circumstances evince a "strong preference" by the government that they do so, as well as an active interest in any resulting investigation. Both Facebook and Yahoo plainly relied on these statutory provisions to access, search, and ultimately disclose communications that are constitutionally protected. This is more than enough to constitute government statutory action under *Skinner*.

Relatedly, searches pursuant to an overarching governmental initiative are government action. *See Davis, supra* (airport search was government action when "part of a nationwide anti-hijacking program conceived, directed, and implemented

by federal officials in cooperation with air carriers"). *See also United States v. Ross*, 32 F.3d 1411, 1413 (9th Cir. 1994) ("The government's involvement in promulgating the Federal Aviation Administration guidelines to combat hijacking is so pervasive "as to bring any search conducted pursuant to that program within the reach of the Fourth Amendment."); *United States v. Vigil*, 989 F.2d 337, 340 (9th Cir. 1993) (same, for search by private security guard at airport metal detector).

Here, the effort to combat child exploitation is a highly regulated, comprehensive federal initiative similar to the anti-hijacking regulations of the 1970s. As the Department of Justice asserts on its own website, "Project Safe Childhood" is a "unified and comprehensive strategy to combat child exploitation."[156] The D.O.J. asserts that it works with a comprehensive network of federal and state law-enforcement agencies and "partners includ[ing] the National Center for Missing and Exploited Children" and others.[157] This federally coordinated effort, while laudable, subjects the resulting searches to Fourth Amendment scrutiny. For this reason too, [redacted] motions to suppress should have been granted.

---

156 *See* https://www.justice.gov/psc/about-project-safe-childhood (last visited June 28, 2020).

157 *Id.*

*c. Even if a legitimate business reason to carry out these searches existed, there was still "government action."*

As set forth above, this Court should find that government action occurred, and it can do so without disturbing the two-pronged test stated in *Miller*. But even beyond the strictures of that test, government action is amply shown on this record. As demonstrated above, government action can result in *any one* of the following circumstances: 1) government acquiescence to unlawful private searches (*Walther* DEA searches; *Reed* hotel search); 2) a private party's intent to facilitate arrests or convictions (*Reed* hotel search); 3) federal statutes that require (or even *permit*) otherwise-unconstitutional private searches (*Skinner* railroad-urinalysis regulations); and 4) overarching government initiative (*Davis, Ross* airport cases). Each of those situations was analyzed above, but importantly, *any* of them result in Fourth Amendment scrutiny, even if the private companies also had legitimate business reasons to carry out these searches. The existence of a business purpose does not strip away Fourth Amendment protections when there is *also* government knowledge and acquiescence to unlawful searches, or an unconstitutional statute, or statutorily encouraged searching, or statutorily permitted searching, or overarching government initiatives, or even—as here—legitimate business interests *combined* with the business's desire to obtain arrests and convictions.

But there was government action for two more reasons also. First, "[i]t is well established" that the Fourth Amendment applies to private searches "if the

government agents instigate it." *United States v. Krell*, 388 F. Supp. 1372, 1374 (D. Alaska 1975). When that occurs, the party becomes a *de facto* agent of the government. *See United States v. Ziegler*, 474 F.3d 1184, 1190 (9th Cir. 2007) ("Given the district court's factual findings [that an officer requested the search] we treat [the private employees] as de facto government agents."). That is what occurred here.

And second, it is also government action if law enforcement participated at any point along the way. "[A] search is a search by a federal official if he had a hand in it ... so long as he was in it before the object of the search was completely accomplished, he must be deemed to have participated in it." *Lustig v. United States*, 338 U.S. 74, 78-79 (1949). "The Fourth Amendment applies to a search whenever the government participates *in any significant way in this total course of conduct.*" *United States v. Davis*, 482 F.2d 893, 896-97 (9th Cir. 1973) (emphasis provided; internal citations and punctuation omitted). In *Corngold v. United States*, 367 F.2d 1, 5-6 (9th Cir. 1966), for example, this *en banc* Court held that when a search is "a joint operation . . . [and] a federal agent participates in such a joint endeavor, the effect is the same as though he had engaged in the undertaking as one exclusively his own." *Id.* (quoting *Byars v. United States*, 273 U.S. 28, 33 (1927) (internal punctuation omitted)). *See also United States v. Young*, 573 F.3d 711, 713 (9th Cir. 2009) (government action where hotel security discovered a gun

in defendant's room, but police accompanied security to the room to retrieve it); *Reed*, 15 F.3d at 932 (police accompanied hotel security to room and "stood lookout" during ostensibly private search).

As described above, the government both instigated and participated in the overall investigation at various points along the way. Analyzing, as we must, the "total course of conduct," this was not an independent private search. As such, it constituted government action, the Fourth Amendment applied, and suppression of the evidence should have resulted.

### C. The government's subpoenas and preservation requests were also illegal searches and seizures under *Carpenter*.

The recent Supreme Court case *Carpenter v. United States*, 138 S. Ct. 2206 (2018) also instructs that [redacted] had a legitimate right to privacy in his digital data, and that it violated the Fourth Amendment to interfere with that right without a warrant and probable cause. In *Carpenter*, the government obtained orders directing wireless carriers to provide cell-tower data regarding several criminal suspects. *Id.* at 2212. The Supreme Court reversed the resulting conviction, holding that warrantlessly obtaining this information violated the Fourth Amendment. In so doing, it rejected the notion that the third-party doctrine insulated this information from Fourth Amendment scrutiny, noting that third-party-doctrine cases did not deal with "confidential communications" and other

private information. *Id.* at 2219.[158] The Court held that a warrant should have been required: "*this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy*" it observed. *Id.* at 2221 (emphasis provided). "If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement." *Id.* at 2222.

*Carpenter* demonstrates that searches and seizures occurred here. The government seized Yahoo records through ongoing preservation requests, with no notice to [redacted] And it both seized property and affirmatively prompted additional searches by issuing administrative subpoenas to Facebook. Under *Carpenter*, this should have required a warrant showing probable cause. Because the government had neither, this evidence should have been suppressed.

**D. The search warrant affidavit failed to show probable cause to search for child pornography.**

Even with all of the illegally obtained chats and communications, the warrant affidavit still lacked probable cause to search for child pornography. To

---

[158] Even the dissent seemed to concede that private communications—as opposed to mere location data—would not be governed by the third-party doctrine. *See id.* at 2230 (Kennedy, J., dissenting) ("*Miller* and *Smith* [the leading third-party cases] may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party.") (citing *Ex parte Jackson*, 96 U. S. 727, 733 (1878) (letters held by mail carrier); *United States v. Warshak*, 631 F. 3d 266, 283-288 (6th Cir. 2010) (e-mails held by Internet service provider)).

demonstrate probable cause that a particular image is child pornography, an agent should either include the image itself, or a reasonable factual description of it. *See United States v. Perkins*, 850 F.3d 1109, 1118-119 (9th Cir. 2017) (where search warrant affiant "merely proffered his own . . . incomplete and misleading description of the image" probable cause was lacking). *See also United States v. Battershell*, 457 F.3d 1048, 1052-53 (9th Cir. 2006) (where warrant does not include copies of alleged contraband, a factual description sufficient to meet the statutory definitions is required). Here, the search warrant affiant claimed that [redacted] was involved in obtaining and distributing child pornography. But the images that the government had received were simply not child pornography—as NCMEC itself had determined. Failing to mention this fact, while asking for a warrant for child pornography, was unlawful under *Perkins* and *Battershell.*

And [redacted] sex-tourism plans overseas, even if involving underage girls, did not automatically provide probable cause for child pornography either. *See United States v. Needham*, 718 F.3d 1190, 1195 (9th Cir. 2013) ("the bare inference that those who molest children are likely to possess child pornography . . . does not establish probable cause to search a suspected child molester's home for child pornography."). *See also Perkins*, 850 F.3d at 1120 (same). Nor do the agent's boilerplate profiling statements in the affidavit add anything to the analysis. *See id.* (rejecting a "boilerplate description of a child pornography

collector, characterized as someone who 'may receive sexual gratification, stimulation, and satisfaction from contact with children'" because "[s]uch a generalized statement, which was not drafted with the facts of this case or this particular defendant in mind, does little to support probable cause") (*quoting United States v. Weber*, 923 F.2d 1338, 1345 (9th Cir. 1990)).

Because the warrant affidavit did not show probable cause that pornography would be found, the motion to suppress should have been granted.

### E. Suppression is the only appropriate remedy for these repeated violations.

Mr. [redacted] convictions should be reversed because they were all fruit of the poisonous tree. The government received the evidence against [redacted] only *after* it learned about Yahoo's illegal searches, and through the same illegality.[159] The Yahoo evidence led directly to the Facebook evidence.[160] The Facebook evidence restarted an otherwise "stalled" investigation, where probable cause had become "stale."[161] Both the Yahoo and the Facebook evidence made up almost the entirety of the purported probable cause in the search warrant. *See* ER 2718-

159 ER 1737-1739; 1777; 1782-1783; 1943; 1957.
160 ER 1912.
161 ER 1905-1906, 1911.

2774.[162] And the fruit of the search warrant evidence was used almost exclusively to convict [redacted] at trial.[163]

When tainted evidence is included in a search-warrant application, a reviewing court must excise the offending portion of the warrant and reevaluate whether it continues to support probable cause. *See United States v. Bishop*, 264 F.3d 919, 924 (9th Cir. 2001). Here, that exercise would gut the affidavit of probable cause almost exclusively, rendering the search warrantless and unlawful.

Nor does the *Leon* good-faith exception save the government here. Though this will no doubt be an argument raised in the answering brief and thus in [redacted] reply, by way of preview, the Court should consider the following:

- The affidavit was based on unlawfully obtained evidence, knowingly included in the search warrant—facts that go to the heart of the exclusionary rule. *Bishop*, 264 F.3d at 924.

- The affidavit untruthfully stated that the offending information was obtained by subpoenas and search warrants, when agents knew that it was the fruit of unlawful extrajudicial searches instead.[164]

---

[162] The case-specific factual allegations in the affidavit are contained at ER 2719-2760. Of those allegations, the Yahoo information comprised paragraphs 7-16; (ER 2720-2729) and the Facebook information made up paragraphs 17-25 (ER 2729-2760).

[163] *See generally*, ER 484-966.

[164] ER 1908 (agent admitting that affidavit inaccurately represented that Yahoo information was from other search warrants); ER 1892 (agent admitting that claim that information was from administrative subpoena was also untrue).

- The search warrant affiant was a straw-man: while he claimed having at least some of his "own personal knowledge"[165] the document was ghost-written by another agent,[166] he had never done any substantive work on the case, even after learning that he would be the substitute affiant,[167] he had no independent knowledge of the facts,[168] and he did not know whether the information in the affidavit had been obtained legally or illegally.[169]

- The affidavit suggested that certain images constituted child pornography when the agent had never viewed them, and they objectively did not.[170]

For all of these reasons, exclusion is the appropriate remedy, and "good faith" is no exception to the usual rule.

## II. The conviction on Count 1 must be reversed, because the jury was improperly instructed on the "purpose" element of 18 U.S.C. § 2251(c).

### A. Standard of Review.

Failure to instruct the jury on an appropriate defense theory is a question of law reviewed de novo. *Stewart v. Ragland*, 934 F.2d 1033, 1042 (9th Cir. 1991). Whether the instructions issued by the district court adequately cover the defendant's theory of the case presents a question of law reviewed *de novo*. *United States v. Warren*, 25 F.3d 890, 895 (9th Cir.1994).

---

165 ER 2719.
166 ER 1850-1851, 1865-1866.
167 ER 1859-1860.
168 ER 1865-1866.
169 ER 1867-1868.
170 ER 1918-1920.

### B. The district court erred by failing to instruct the jury that the prohibited "purpose" was a *but-for* cause of the defendant's actions.

Title 18 U.S.C. § 2251(c)(1) creates felony liability for anyone who "persuades, induces, [or] entices, or coerces any minor to engage in . . . any sexually explicit conduct outside of the United States"—but does so only when the conduct is "*for the purpose of* producing any visual depiction of such conduct." *Id.* (emphasis provided). [redacted] testified that his sexual conduct in the Philippines was simply for his own personal gratification, and that producing a visual depiction of the same was not what motivated him to have the sexual encounters.[171]

[redacted] proposed that, consistent with *Burrage v. United States*, 134 S. Ct. 881, 888-90 (2014), "purpose" be defined as including a "but-for" causation instruction. CR 126 at 4. That is, he asked the jury to be instructed that the government must prove that he would not have taken the given action (the sexual conduct) *but-for* the illicit purpose (making a visual depiction).[172] It was error to deny that instruction, for the reasons that follow.

---

171 ER 567.

172 For Count One, the action would be engaging in sexually explicit conduct with the minor; the purpose would be to create a visual depiction of the same. For Count Two, the action would be international travel; the purpose would be engaging in illicit sexual conduct.

### *1. Under Burrage, "purpose" should require "but-for" causation.*

The argument for applying *Burrage*'s "but-for" instruction boils down to a syllogism:

- Under Supreme Court precedent, statutes that require a certain *motive* require *"but-for" causation* instructions.
- *"For the purpose of,"* as used in Counts One and Two, is a *motive* requirement.

Therefore:

- *"For the purpose of,"* as described in § 2251, requires a *"but-for" causation* instruction.

#### *a) Under Supreme Court precedent, elements that require a certain "motive" must be subjected to "but-for" causation analysis.*

*Burrage* held that a criminal drug statute that punished "death or serious bodily injury result[ing] from" a drug offense required "but-for" causation between the criminal act and the death that was alleged to be "resulting." 571 U.S. at 211 ("[t]his but-for requirement is part of the common understanding of cause.").

But in so doing, it clarified that under its own precedent, *but-for* causation is also required whenever a specific *motive* is an element of a claim or offense. This makes sense, because "motive" is perhaps best thought of as the "cause" of a person's actions. And the cases consistently require a "but-for" jury instruction when a defendant's motive is at issue. In *Safeco Ins. Co. of Am. v. Burr*, 551 U.S.

47, 63-64 (2007), for example, the Court reviewed a statute that prohibited "adverse action" by an insurance company "based on" consumer credit reports. The Court held that the statutory claim required a *but-for* relationship between the review of the credit reports and the adverse action taken. *See id.* ("the phrase 'based on' indicates *a but-for causal relationship* and thus a necessary logical condition. Under this most natural reading of [the statute] then, an increased rate is not 'based in whole or in part on' the credit report unless the report was *a necessary condition* of the increase.") (emphasis provided).

The same was true in *Gross v. FBL Fin. Servs.*, 557 U.S. 167, 180 (2009). There, the Court held that to prove that employment action was *motivated* by an discriminatory factor, *but-for* causation was required. *See id.* ("a plaintiff bringing a disparate-treatment claim pursuant to the ADEA must prove, by a preponderance of the evidence, that age *was the 'but-for' cause of the challenged adverse employment action*.") (emphasis provided).

Similarly, when a statute "makes it unlawful for an employer to take adverse employment action against an employee 'because' of certain criteria" that "require[s] proof that *the desire to retaliate was the but-for cause* of the challenged employment action." *Univ. of Tex. Sw. Med. Ctr. v. Nassar*, 570 U.S. 338, 352 (2013) (emphasis provided).

It was this Supreme Court precedent governing motive and causation that persuaded the Sixth Circuit to apply *Burrage* to a hate-crime statute in *United States v. Miller*, 767 F.3d 585, 592 (6th Cir. 2014). In short, *Miller* held: "[t]he prohibited . . . motive must be an actual cause of the specified outcome." *Id.* (reversing conviction). "That conclusion makes good sense in the context of a criminal case implicating the motives of the defendants." *Id.*

*b) "For the purpose of" means motive.*

Thus, when motive is at issue, but-for causation is required. Setting aside for a moment what the proper definition should be, it cannot be disputed that "*for the purpose of*" describes a defendant's motive. The Supreme Court's seminal "purpose" case, *Mortensen v. United States*, 322 U.S. 369 (1944), made that clear. There, the Supreme Court held that the "*for the purpose of*" element of a Mann Act prosecution required that that the illicit purpose "be the dominant *motive* of such interstate movement." 322 U.S. at 374. Even courts that have watered *Mortensen* down (to require something less than "*the*" dominant motive) still recognize that "purpose" equates to *a* "motive." *See, e.g., United States v. Ellis*, 935 F.2d 385, 390 (1st Cir. 1991) (upholding instruction requiring that criminal sexual activity be "one of the several *motives* or purposes"); *United States v. Campbell*, 49 F.3d 1079, 1083 (5th Cir. 1995) ("many purposes for traveling may exist, but, as long as

one *motivating purpose* is to engage in prostitution, criminal liability may be imposed under the Act").

Thus, the syllogism holds true:

1) Supreme Court precedent is clear that questions of motive boil down to but-for causation: would the defendant have taken the action but-for the prohibited motivation? *See Gross,* 557 U.S. at 180; *Nassar*, 570 U.S. at 352; *Burr*, 551 U.S. at 63-64; *Miller*, 767 F.3d at 592.

2) "For the purpose of" describes motive. *Mortensen,* 322 U.S. at 374. *Ellis*, 935 F.2d at 390 (describing "*motives* or purposes"); *Campbell*, 49 F.3d at 1083 ("*motivating purpose"*); *United States v. Sirois*, 87 F.3d 34, 39 (2d Cir. 1996).

Therefore:

3) The jury should have been instructed that to prove these elements, the act (either causing a minor to engage in sexually explicit conduct in Count One, or international travel in Count Two) would not have occurred *but-for* the forbidden purpose (the intent to create a visual depiction in Count One, or the desire to engage in illicit sexual conduct in Count Two).

Supreme Court precedent, and Due Process, require no less.

### 2. *But-for causation is appropriate because "purpose" is the most stringent mens rea in criminal law.*

It is appropriate to require but-for causation because "purpose" is the highest mental state in criminal law—tantamount to specific intent. *See, e.g., United*

*States v. Gracidas-Ulibarry*, 231 F.3d 1188, 1196 (9th Cir. 2000) (en banc) (observing that "[t]he confusion between general and specific intent has been the catalyst for a movement to replace these categories with a hierarchy of four levels of culpable states of mind, defined with greater clarity: purpose, knowledge, recklessness and negligence" and that "[i]n general, 'purpose' corresponds to the concept of specific intent, while 'knowledge' corresponds to general intent.").

Indeed, in the Model Penal Code—which was also used as an additional resource by the Supreme Court in *Burrage*—"purpose" is used to refer to the highest level of criminal culpability (followed by knowledge, recklessness, and negligence). Requiring the fact-finder to discern the accused's actual "purpose" in acting is simply not a foreign concept in criminal law. In *Haupt v. United States*, for example, the Supreme Court confirmed that it was for the jury to decide the defendant's "purpose" in acting: that is, if Haupt was guilty of treason because his "purpose [was] to aid and comfort the enemy" or if he was simply a father who had the "misfortune to sire a traitor." 330 U.S. 631, 636 (1947).

It makes sense that Congress intended to require "but-for" causality in selecting the "for the purpose of" language of 18 U.S.C. § 2251(c) because the Act creating this offense was targeted specifically at the harm of "production" of child pornography. The section of the PROTECT Act creating § 2251(c) as it now exists was entitled "Extraterritorial Production of Child Pornography for Distribution in

the United States." Pub. L. 108-21, 117 Stat. 683 (Apr. 20, 2003). It was designed to "prosecute foreign producers of child pornography." H. Rept. 108-66 at 62 (Apr. 9, 2003). And the "purpose of th[e] section" was described as to "stop efforts by producers of child pornography to avoid criminal liability based on the fact that the child pornography was produced outside of the United States, *but intended for use inside the United States.*" *Id*. at 62-63 (emphasis provided).

If Congress had wanted § 2251(c) to sweep more broadly and intended to require something less than "but-for" causation, it could have simply omitted "for the purpose of" language entirely and instead criminalized (1) enticing a minor to engage in "sexually explicit conduct" (2) while "producing any visual depiction of such conduct" or with knowledge that "any visual depiction of such conduct" would be produced when (3) the person intends for the visual depiction to be transported into the United States. But the statute continues to require purpose, and "purpose" means but-for causation. Failure to instruct accordingly was error.

**3. The rule of lenity also calls for the but-for test.**

If there is any doubt as to the proper definition of "purpose," the rule of lenity states that it be resolved in a defendant's favor. *See United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012). Indeed, even Justices who opposed *but-for* causation in a civil setting, *cf. Nassar*, 133 S. Ct. at 2546 (Ginsburg, J., dissenting), agree that it is required for a criminal conviction. *See Burrage*, 134 S. Ct. at 892

(Ginsburg, J., joined by Sotomayor, J., concurring in the judgment) ("in the interpretation of a criminal statute subject to the rule of lenity, where there is room for debate, one should not choose the construction that disfavors the defendant.") (internal quotations omitted).

If there was any doubt as to the definition of purpose, that doubt should inure to the defendant's benefit. For this reason too, the district court erred.

## III. [redacted] Sentencing Guidelines' range was erroneously increased by a "multiple-count" adjustment that is improper for § 2252 offenses.

[redacted] was convicted of only one count under § 2252(a), yet the court ultimately punished him as if he had been convicted of four separate counts. In *United States v. Chilaca*, 909 F.3d 289, 292 (9th Cir. 2018), this Court analyzed whether under § 2252(a)(4)(B) "simultaneous possession of child-pornography images, stored in different media and found in the same location, creates separate 'allowable units of prosecution.'" It held that Congress intended "§ 2252(a)(4)(B)'s use of the phrase '1 or more' to mean that the simultaneous possession of different matters containing offending images at a single time and place constitutes a single violation of the statute." *Id*. at 295.

Sentencing [redacted] as if he had been indicted on, and convicted of, four separate violations of § 2252, something not envisioned by Congress nor permitted by Ninth Circuit precedent, was error. In addition to the Fifth Amendment concerns addressed in *Chilaca*, it also violates the Sixth Amendment as set forth in

*Apprendi v. New Jersey*, 530 U.S. 466 (2000) and *Alleyne v. United States*, 570 U.S. 99 (2013). Because the jury in this case did not make any special findings as to Count 3, *see* ER 448-449, the trial court should not have been allowed to rely on its own factfinding to increase the Guideline range to 50 years as recommended in the PSR. Procedural error resulted.

## Conclusion

The government is right to investigate and prosecute child exploitation offenses. And it is understandable for internet service providers to seek to help in that endeavor. But the government, and the companies that it interacts with, must do so constitutionally. Because while a small minority of persons may seek to commit serious online crimes, *all* Americans are entitled to the Fourth Amendment's protection of their digital papers and effects. This Court cannot tolerate warrantless searches that merely deputize private parties to do what the government cannot. Accordingly, this Court should hold that the searches in this case amounted to government action, and vacate the convictions that relied on them.

Dated: June 29, 2020

Respectfully submitted,

*s/ Timothy A. Scott*

TIMOTHY A. SCOTT
SCOTT TRIAL LAWYERS, APC
Attorneys for [redacted]

## Statement of Related Cases

Counsel is not aware of any cases pending before this Court that are related to this matter.

Dated: June 29, 2020

*s/ Timothy A. Scott*
TIMOTHY A. SCOTT
Attorney for [redacted]

# UNITED STATES COURT OF APPEALS
# FOR THE NINTH CIRCUIT

## Form 8. Certificate of Compliance for Briefs

*Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf*

**9th Cir. Case Number(s)** [redacted]

I am the attorney or self-represented party.

**This brief contains** 13,984 **words**, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- (•) complies with the word limit of Cir. R. 32-1.
- ( ) is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ( ) is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ( ) is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ( ) complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one):*
  - ( ) it is a joint brief submitted by separately represented parties;
  - ( ) a party or parties are filing a single brief in response to multiple briefs; or
  - ( ) a party or parties are filing a single brief in response to a longer joint brief.
- ( ) complies with the length limit designated by court order dated [ ].
- ( ) is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

**Signature** s/ Timothy A. Scott **Date** 6/29/2020

*(use "s/[typed name]" to sign electronically-filed documents)*

*Feedback or questions about this form? Email us at forms@ca9.uscourts.gov*

# UNITED STATES COURT OF APPEALS
# FOR THE NINTH CIRCUIT

## Form 15. Certificate of Service for Electronic Filing

*Instructions for this form: http://www.ca9.uscourts.gov/forms/form15instructions.pdf*

**9th Cir. Case Number(s)** [redacted]

I hereby certify that I electronically filed the foregoing/attached document(s) on this date with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit using the Appellate Electronic Filing system.

**Service on Case Participants Who Are Registered for Electronic Filing:**

☐ I certify that I served the foregoing/attached document(s) via email to all registered case participants on this date because it is a sealed filing or is submitted as an original petition or other original proceeding and therefore cannot be served via the Appellate Electronic Filing system.

**Service on Case Participants Who Are NOT Registered for Electronic Filing:**

☐ I certify that I served the foregoing/attached document(s) on this date by hand delivery, mail, third party commercial carrier for delivery within 3 calendar days, or, having obtained prior consent, by email to the following unregistered case participants *(list each name and mailing/email address)*:

**Description of Document(s)** *(required for all documents)*:

Appellant's Opening Brief

**Signature** s/ Timothy A. Scott **Date** 6/29/2020

*(use "*s/[typed name]*" to sign electronically-filed documents)*

*Feedback or questions about this form? Email us at forms@ca9.uscourts.gov*