United States Court of Appeals
For the First Circuit

No. 11-1275

UNITED STATES OF AMERICA,

Appellee,

v.

JAMES M. CAMERON,

Defendant, Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MAINE

[Hon. John A. Woodcock, U.S. District Judge]

Before

Torruella, Howard, and Thompson,
Circuit Judges.

Peter Charles Horstmann, with whom Partridge, Ankner & Horstmann, was on brief for appellant.

Anthony Vitarelli, Assistant United States Attorney, Criminal Division, Appellate Section, with whom Lanny A. Breuer, Assistant Attorney General, John D. Buretta, Acting Deputy Assistant Attorney General, Thomas E. Delahanty II, United States Attorney, and Margaret D. McGaughey, Assistant United States Attorney, was on brief for appellee.

November 14, 2012

TORRUELLA, Circuit Judge. Following a bench trial in the U.S. District Court for the District of Maine, Defendant-Appellant James M. Cameron ("Cameron") was convicted of thirteen counts for crimes involving child pornography. Cameron now appeals, challenging various rulings by the district court before and after the trial. The challenged rulings include: (1) the denial of a motion to dismiss the indictment for insufficiency and for improper venue, United States v. Cameron (Cameron I), 662 F. Supp. 2d 177 (D. Me. 2009); (2) the denial of a motion to suppress evidence allegedly seized in violation of the Fourth Amendment, United States v. Cameron (Cameron II), 729 F. Supp. 2d 418 (D. Me. 2010); (3) the denial of a motion in limine to exclude certain evidence on Confrontation Clause grounds, United States v. Cameron (Cameron III), 733 F. Supp. 2d 182 (D. Me. 2010); and (4) the calculation of the number of child pornography images attributable to Cameron for sentencing purposes.

This case presents complex questions of first impression in this Circuit regarding the admissibility of evidence in the wake of the Supreme Court's recent Confrontation Clause jurisprudence. After careful review, we conclude that the admission of certain evidence violated Cameron's Confrontation Clause rights. We further conclude that the admission of this evidence was harmless as to some counts of conviction (Counts Six, Seven, Nine, Ten, Twelve, Thirteen, and Fifteen), but not as to others (Counts One,

Three, Four, Five, Eleven, and Fourteen). We thus reverse Cameron's convictions on certain counts and remand for re-sentencing, or a new trial if the government wishes to so proceed.

I. Background

A. Business and Regulatory Background

Before delving into the particular facts of Cameron's case, we recite some background facts regarding the technologies, business practices, and regulations at issue here.

During 2006 and 2007, Yahoo!, Inc. ("Yahoo!") offered a service (which has since been discontinued) called "Yahoo! Photo" that allowed users to upload photographs to the Internet. Users could then share photographs with other Yahoo! Photo users. Each Yahoo! Photo album was linked to a particular Yahoo! "user" or "account." In turn, each "account" was designated by a "Login Name" (sometimes referred to as a "username" or "screen name"), such as "lilhottee00000," one of the screen names at issue in this case. A Yahoo! user might use multiple other Yahoo! services in addition to Yahoo! Photo, such as email.

Whenever a person created a Yahoo! account, Yahoo! recorded certain information, some of which was captured automatically and some of which was entered by the person who created the account. One piece of information that was automatically collected was the "Registration IP Address," which was the Internet Protocol ("IP") address from which the account was

created.[1] Yahoo! also automatically recorded the date and time at which the account was created. Yahoo! recorded this information in an "Account Management Tool," which it maintained for the life of a Yahoo! account. Further, whenever a user logged into a Yahoo! account, Yahoo! automatically recorded the date and time of the login as well as the IP address from which the login occurred. Yahoo! stored this information in a "Login Tracker." The record indicates that, during the relevant time period, Yahoo! kept login records in its Login Tracker for sixty days.

During the same time period, Google, Inc. ("Google") provided a service (also since discontinued) called "Google Hello." Google Hello allowed users to sign in with a username and then chat and trade photos with other users over the Internet. Google automatically maintained records indicating the times at which a user logged into and out of Google Hello, as well as the IP address from which the user accessed the service ("Google Hello Connection Logs").

At the relevant time, businesses such as Google and Yahoo! had (and still have to this day) a duty to report any apparent violation of federal child pornography laws to the National Center for Missing and Exploited Children ("NCMEC"). See

[1] "An IP address is the unique address assigned to every machine on the internet. An IP address consists of four numbers separated by dots, e.g., 166.132.78.215." United States v. Kearney, 672 F.3d 81, 84 n.1 (1st Cir. 2012) (quoting United States v. Vázquez-Rivera, 665 F.3d 351, 354 n.5 (1st Cir. 2011)).

42 U.S.C. § 13032(b)(1) (1998) (creating a reporting duty for any entity "engaged in providing an electronic communication service or a remote computing service to the public, through a facility or means of interstate or foreign commerce") (current version at 18 U.S.C. § 2258A(a)(1) (2012)). NCMEC is a non-profit organization that receives an annual grant from Congress to perform various functions related to preventing the exploitation of children. See 42 U.S.C. § 5773(b) (2012). Among these functions is the operation of a "cyber tipline to provide . . . electronic service providers an effective means of reporting" child pornography and other Internet-related crimes targeting children. Id. § 5773(b)(1)(P). NCMEC's "cyber tipline" is called the "CyberTipline." Once NCMEC receives a report of a possible child pornography crime via the CyberTipline, it determines "the appropriate international, Federal, State or local law enforcement agency for investigation" and forwards the report to that agency. Id.

B. Yahoo! Reports to NCMEC

On March 15, 2007, Yahoo! received an anonymous report that child pornography images were contained in a Yahoo! Photo account belonging to a user with the username "lilhottyohh." The record does not indicate that Yahoo! knew, or ever attempted to find out, who made the anonymous report. In response to the anonymous tip, Yahoo! personnel searched the "lilhottyohh" account

and discovered images that they believed to be child pornography. It is not known which Yahoo! employee conducted the search.

Yahoo! had an established process for dealing with reports of child pornography. If Yahoo! learned of child pornography in an account, an employee in Yahoo!'s Customer Care Department temporarily removed the content from public view and reviewed it. If he or she determined that the account contained child pornography, Yahoo! deactivated the account and notified the Legal Department. Meanwhile, the Customer Care Department created an archive of all the images associated with the account, including the date and time each image was uploaded and the IP address from which it was uploaded. If the Legal Department agreed that any images were child pornography, it then sent an electronic report to NCMEC via the CyberTipline. Each report ("Yahoo! CP Report" or "CP Report") listed a "Suspect Screen Name," a "Suspect Email Address," a "Suspect URL,"[2] and a "Suspect IP Address." The "Suspect IP Address" was the IP address that Yahoo! "associated" with the user; it is not clear from the record whether this IP address was the "Registration IP Address" stored in the Account Management Tool, or

[2] For the purposes of this case, we understand a Uniform Resource Locator ("URL") to be the string of characters that specifies the location of a document on the Internet. For example, the URL for the First Circuit's website (at the time of this writing) is "http://www.ca1.uscourts.gov". URLs are distinct from IP addresses. An IP address identifies a particular computer on the Internet, but that computer might host multiple documents, each of which might have their own URL.

if it was some other IP address. One could argue, as the government seemed to do at trial, that it is the IP address from which the last image was uploaded onto the account, as in some CP Reports the "Suspect IP Address" is different from the "Registration IP Address" contained in the Account Management Tool for the same account. The "Suspect Email Address" was the Yahoo! email address of the Yahoo! user the CP Report pertained to, and the "Suspect URL" was the Internet location where the user's photos could be found.

Each CP Report also included a table listing the child pornography images being sent with the report. Yahoo! attached to each report the suspected child pornography images. For each child pornography image, Yahoo! listed the date and time at which the image was uploaded and the IP address from which it was uploaded ("Image Upload Data"). In addition, Yahoo attached data from the Account Management Tool and Login Tracker to each CP Report. Whenever Yahoo! sent a CP Report to NCMEC, Yahoo! automatically stored a receipt. The receipt included a unique number assigned to the report by NCMEC and a record of what Yahoo! reported to NCMEC, including the attachments to the CP Report.

In this case, Yahoo! sent a CP Report of the child pornography in the "lilhottyohh" account to NCMEC. Subsequently, Yahoo! sent additional CP Reports to NCMEC of child pornography found in the accounts of the users "lilhottee0000" and

"harddude0000." All three CP Reports listed the same "Suspect IP Address": 76.179.26.185.

C. ICAC Seizes Cameron's Computers

On August 3, 2007, NCMEC sent a report ("CyberTipline Report") of child pornography found in the "lilhottee00000" Yahoo! account to the Maine State Police Internet Crimes Against Children ("ICAC") unit. NCMEC later sent another CyberTipline Report to ICAC, this time regarding child pornography found in the Yahoo! Photo account of user "harddude0000." Both CyberTipline Reports listed the same IP Address, 76.179.26.185, in the "Suspect Information" section. Each report also noted that "[t]he IP included in this report is the most recent file or image upload IP available," and then listed the date and time of the most recent upload.[3]

ICAC detective Laurie Northrup ("Northrup") determined that the IP address 76.179.26.185 was part of a pool of IP addresses that Time Warner, an Internet Service Provider ("ISP"), distributed to its Internet access customers. Through a subpoena to Time Warner, Northrup determined that the IP address

[3] Moreover, the IP Address contained in each of the CyberTipline Reports matched the "Suspect IP Address" contained in its corresponding Yahoo! CP Report, although we do not know whether this is by pure coincidence or if both IP Addresses really refer to the computer that originated the most recent image upload. As we mentioned earlier, the Yahoo! CP Reports did not state whether the "Suspect IP Address" contained therein was the one from which the most recent image had been uploaded, a representation which was in fact made by in the CyberTipline Reports.

76.179.26.185 had been assigned to the Cameron residence in Hallowell, Maine during the relevant time periods. On December 21, 2007, Maine police executed a search warrant at the Cameron residence. Officers found four computers at the residence: a Compaq desktop, a Dell laptop, an HP desktop with an external hard drive, and an eMachines desktop with an external hard drive. ICAC also executed a search warrant at Cameron's workplace and seized his office computer. ICAC's preliminary examination of the computers in Cameron's home (conducted on site) indicated possible child pornography on the HP desktop. This examination also indicated that certain Yahoo! accounts had been accessed from the eMachines computer. Northrup later requested information from NCMEC related to these accounts.

In March of 2008, forensic examiner Scott Bradeen ("Bradeen") examined Cameron's five computers and external hard drives. For each computer, Bradeen determined the IP addresses from which the computer had accessed the Internet. Bradeen found evidence that someone had accessed seventeen different Yahoo! accounts, including those that were the subject of the reports that NCMEC originally sent to ICAC, from various computers in Cameron's home. In addition, Bradeen found child pornography images and transcripts indicating that someone using Cameron's computers had signed into Google Hello using one or more usernames to send and receive child pornography images. Bradeen found child pornography

images on Cameron's Dell laptop and on his HP desktop. Bradeen found no child pornography on the Compaq desktop or on the eMachines desktop. However, the Internet history stored on the eMachines desktop showed that someone had executed Internet searches for terms related to child pornography.

D. ICAC Search Warrants to Yahoo! and Google

ICAC subsequently served search warrants on Yahoo! for information about the Yahoo! accounts that had been accessed from Cameron's computers. The data produced by Yahoo! in response to the search warrants included emails that had been sent to and from those accounts. The emails indicated that on at least one occasion, someone using the "harddude0000" Yahoo! account sent child pornography to another individual via email and received child pornography via email in response. Yahoo! also produced the receipts of its Yahoo! Reports to NCMEC, the "Account Management Tool," and the "Login Tracker" for each account; however, it is not clear if Yahoo! produced the Image Upload Data. In addition, Yahoo! produced disks containing images of child pornography found in the accounts in question.

ICAC also served search warrants on Google for information regarding the Google Hello accounts accessed from Cameron's computers. In response, Google provided the Google Hello Connection Logs for the specified user accounts.

E. Indictment and Pre-Trial Proceedings

On February 11, 2009, a federal grand jury indicted Cameron on sixteen counts of child pornography-related crimes. The counts included ten counts of knowingly transporting child pornography in violation of 18 U.S.C. §§ 2252A(a)(1) and 2256(8)(A); four counts of knowingly receiving child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) and 2256(8)(A); and two counts of knowingly possessing child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2256(8)(A). Each of the counts recited a specific date on which Cameron allegedly transported, received, or possessed child pornography. Of the ten counts of transporting child pornography, seven alleged the uploading of child pornography images to Yahoo! Photo accounts; two alleged the sending of child pornography via Google Hello; and one alleged both the uploading of child pornography to Yahoo! Photos and the sending of child pornography via Google Hello. Of the four counts of receiving child pornography, three alleged that Cameron had received child pornography via Google Hello, and one alleged that Cameron had received child pornography via a Yahoo! email account. All of the transportation counts alleging uploads to Yahoo! Photo specified the Yahoo! usernames Cameron allegedly used. The indictment further alleged that all of the crimes charged occurred in the District of Maine.

Cameron filed three motions prior to trial that are relevant to this appeal. First, on May 18, 2009, Cameron moved to dismiss all counts of the indictment. See Cameron I, 662 F. Supp. 2d at 179. Cameron made a host of arguments, two of which demand our attention here. The first was that all counts of the indictment should be dismissed for insufficient pleading. Specifically, Cameron argued that dismissal was warranted because the indictment did not specify the images that were alleged to be child pornography. Id. at 180. The district court rejected this argument, holding that the indictment satisfied the First Circuit's specificity requirement because each count of the indictment tracked the statutory language and set forth the elements of the offense. Id. at 181 (citing United States v. Sepúlveda, 15 F.3d 1161, 1192 (1st Cir. 1993); United States v. Serino, 835 F.2d 924, 929 (1st Cir. 1987)). Cameron also argued that venue in Maine was improper for three counts because he was not in Maine on the dates of the alleged offenses. Id. at 182-183. The court found that venue was proper because the indictment alleged that the child pornography images on which those counts were based had moved into Maine at some point. Id. at 183. See also 18 U.S.C. § 3237(a) (venue is proper in any district where the offense was started, continued, or completed).

Second, on July 2, 2010, Cameron moved to suppress all evidence resulting from Yahoo!'s searches for child pornography in

Yahoo! Photo accounts that occurred before Yahoo! received search warrants from ICAC. See Cameron II, 729 F. Supp. 2d at 419. Cameron contended that Yahoo! acted as an agent of the government when it searched password-protected accounts for child pornography before reporting to NCMEC. Therefore, Cameron argued, the searches violated his Fourth Amendment rights. Furthermore, Cameron contended that because these allegedly illegal searches were the basis of Yahoo!'s CP Reports to NCMEC, and because NCMEC's resulting CyberTipline Reports to ICAC started the government's investigation, all evidence seized by ICAC should be suppressed as well.

The district court rejected Cameron's argument because it found that Yahoo! had not acted as a government agent. See id. at 422-23. Relying on this court's three-part test from United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009), to be discussed further infra, the district court held that because Yahoo! voluntarily searched the accounts for its own interests and without direction by the government, it did not act as a government agent. Cameron II, 729 F. Supp. 2d at 423-24. The court noted that in a similar case, the Fourth Circuit held that an online email provider did not act as a government agent when it searched the defendant's emails for child pornography and reported it to NCMEC. Id. (citing United States v. Richardson, 607 F.3d 357, 363-67 (4th Cir. 2010)).

Finally, also on July 2, 2010, Cameron filed a motion in limine to exclude all images and other material provided by Yahoo!, Google, and NCMEC. Cameron III, 733 F. Supp. 2d at 183. The government had indicated that it did not intend to call as witnesses the original authors of the Yahoo! Reports to NCMEC, NCMEC's CyberTipline Reports to ICAC, or the Yahoo! records that were attached to the Yahoo! Reports (and then forwarded to ICAC with the CyberTipline Reports) or produced in response to search warrants. Based on this absence of witnesses, Cameron argued that the introduction of this evidence would violate his rights under the Confrontation Clause of the Sixth Amendment. Id. at 185.[4]

The district court denied Cameron's motion without prejudice. The court noted that the Confrontation Clause was implicated only if the prosecution sought to introduce "testimonial" statements without making the declarant available for cross-examination. Id. at 186 (citing United States v. Figueroa-Cartagena, 612 F.3d 69, 84 (1st Cir. 2010)). However, in Crawford v. Washington, the Supreme Court suggested that "business records" were not considered "testimonial." 541 U.S. 36, 56 (2004). Thus, the court considered whether the records in question could be admitted as "business records" under Fed. R. Evid. 803(6). The

[4] The government made a similar representation with respect to the Google records, and Cameron raised a similar challenge. Because Cameron's argument regarding the Google records was identical to his argument for the Yahoo! records, the district court focused its discussion on the Yahoo! records. See id. at 185 n.3.

court held that as long as the government could successfully authenticate the Yahoo! records and establish that they were kept in the ordinary course of business, they would be admissible as business records, and, therefore, the Confrontation Clause would not be implicated. Cameron III, 733 F. Supp. 2d at 188-89. The court also ruled that the NCMEC reports and attached images were admissible as business records because NCMEC simply forwarded information it received from Yahoo!, information which itself consisted of business records. Id. at 189.

F. Trial

Cameron requested a bench trial, which began on August 16, 2010. The government voluntarily dismissed one of the two possession counts before trial. At trial, the government introduced evidence from Yahoo! via the testimony of Christian Lee ("Lee"), a Yahoo! employee. Lee was a Legal Assistant in Yahoo!'s Legal Compliance Department who had no technical training, but who testified that he was knowledgeable about Yahoo!'s data retention and legal procedures. Lee testified about the information that Yahoo! kept about its users. See Part I.A. In particular, Lee stated that Yahoo! automatically recorded the data in the Account Management Tool and the Login Tracker in the regular course of its business in order to "provide reliable and accurate data about its customer accounts." Lee also testified that, as part of its ordinary business practice, Yahoo! automatically stored a receipt

of each CP Report it sent to NCMEC, as well as the attachments, including the Image Upload Data.

Moreover, despite Cameron's objection, the government introduced the Account Management Tool data, the Login Tracker data, and the receipts of Yahoo's CP Reports to NCMEC. The government also introduced compact discs containing the child pornography found in various accounts and other data, including emails, produced in response to the search warrants. However, it does not appear from the record that the government introduced the Image Upload Data (or that the government even had this data).[5]

The government introduced the Google Hello Connection Logs through the testimony of Google employee Colin Bogart ("Bogart"). Bogart was an employee in Google's Legal Compliance Department and, like Lee, had no technical training. Bogart testified that he retrieved the Google Hello Connection Logs by using an internal Google program that allowed him to enter a username and retrieve the Logs for that username. Bogart testified that Google recorded this login information automatically and that it relied on this information for its regular business activities.

---

[5] The information contained in the Image Upload Data, which reflected the date and time each child pornography image was uploaded onto the internet, was central to the government's case-in-chief, as it was the only evidence it could have relied on to prove that Cameron uploaded those images on the specific dates and times alleged in the indictment. The only other piece of evidence that partially contained this information was the NCMEC CyberTipline Reports.

The government introduced the NCMEC CyberTipline Reports through the testimony of John Shehan ("Shehan"), the executive director of NCMEC. Shehan testified that once a report is received through the CyberTipline, NCMEC's staff reviews the suspected images and conducts an online search regarding the provided suspect information. According to him, this query is aimed at identifying the appropriate law enforcement agency with jurisdiction to investigate the suspected child pornography activity. Although NCMEC does not alter the information it receives via the CyberTipline in any way -- other than to record a unique "report ID" and an "entry date," -- Shehan noted that sometimes NCMEC employees would annotate the CyberTipline Reports with their own analysis regarding the information contained therein.[6]

In the instant case, each time a NCMEC employee finished processing the information contained in a Yahoo! CP Report, he or she would create a CyberTipline Report and forward it to the appropriate law enforcement agency, here the ICAC Unit belonging to the Maine State Police. As we briefly described earlier, the CyberTipline Reports received by ICAC contained several sections, among them a "Reporting Person Information" section which reflected Yahoo!'s contact information, as well as a "Suspect Information" section, which provided the user name, e-mail and IP Address of the

[6] The record reflects that these analyses were apparently blocked out, redacted or deleted from the CyberTipline Reports that the government introduced into evidence at trial.

account associated with the images. According to the reports themselves, the IP Address was that of the computer that originated the most recent image file upload. It is unclear exactly how NCMEC extracted this IP Address or how it determined the date and time of the last image upload, information which also appeared on the reports. The only logical conclusion we can draw from the record is that someone at NCMEC analyzed the Image Upload Data attached to the Yahoo! CP Reports and selected the IP address from which the most recent image had been uploaded, along with the date and time of the upload, and included this information in the CyberTipline Report. As we will see later on, this is of particular import to Cameron's argument that the admission of these reports violated his rights under the Confrontation Clause.

Armed with these CyberTipline Reports, ICAC detectives were eventually able to obtain several search warrants against Cameron's home and office. The government introduced evidence regarding what ICAC found through these searches via the testimony of Bradeen and Northrup. Bradeen testified about the child pornography he found on Cameron's computers and about the evidence he found showing that various Yahoo! and Google Hello accounts had been accessed from those computers. Bradeen also testified about the IP addresses from which Cameron's computers had accessed the Internet. Some of these IP addresses matched the IP addresses included in the CyberTipline Reports that NCMEC had created for the

different Yahoo! accounts. For example, there was evidence that all four computers seized at Cameron's home had accessed the Internet at some point through IP address 76.179.26.185, which was the IP address listed on CyberTipline Reports for "lilhottee00000" and "harddude0000." Bradeen also testified that Cameron's HP desktop had accessed the Internet through IP address 24.198.90.108, which the Google Hello evidence showed was an IP address from which a Google Hello user had logged in to trade child pornography.

Additionally, the government introduced evidence showing that, on the specific dates of the transportation and receipt crimes charged in the indictment, Cameron's computers had been assigned the IP addresses from which those crimes had been committed. For example, through a witness from Time Warner, Cameron's ISP, the government introduced records showing that the Time Warner account for Cameron's residence had been assigned certain IP addresses on certain dates. To show that child pornography had actually been uploaded on the dates alleged in the indictment, and to show that it had been uploaded from the IP address that Cameron had on those dates, the government relied on the CyberTipline Reports; it does not appear from the record that the government introduced the Image Upload Data into evidence (or even that it had this information in the first place). The government also introduced extensive evidence to show that no one else living in Cameron's household at the time (Cameron lived with

his wife and two minor children) could have committed the offenses in the indictment.

To show that the images alleged to be child pornography did in fact depict minors, the government relied on the testimony of Dr. Lawrence Ricci ("Ricci"), a physician and child abuse expert. Ricci analyzed the images by determining into which "Tanner Stage" the persons depicted in the images fell. There are five "Tanner Stages" of "secondary sexual development," the first being Stage I, at which there is no evidence of such development. Ricci analyzed the images recovered from Cameron's computers "very conservatively" and identified as minors only those persons whom he considered to be at Stage I, even though children generally reach Stage II between the ages of ten and fourteen.

G. Conviction and Sentencing

Following the bench trial, the district court found Cameron guilty of eight counts of transporting child pornography, four counts of receiving child pornography, and one count of possessing child pornography. The court found Cameron not guilty on two of the transportation counts -- one related to the uploading of photos to Yahoo! Photo and one relating to the sending of photos over Google Hello -- because the court could not conclusively find that the persons in the images connected to those counts were minors. Cameron filed a motion for new trial, in which he renewed his Confrontation Clause arguments, but the district court rejected

that motion. See United States v. Cameron (Cameron IV), 762 F. Supp. 2d 152, 159-60, 165 (D. Me. 2011).

The court sentenced Cameron to 192 months in prison, followed by ten years of supervised release. The sentence was based in part on the court's calculation that Cameron's offenses involved "at least 300, but fewer than 600" images of child pornography, which triggered a sentence enhancement under the United States Sentencing Guidelines ("Guidelines"). See U.S.S.G. § 2G2.2(b)(7)(C) (2012).

Cameron now appeals his conviction and sentence.

II. Discussion

On appeal, Cameron again raises many of the challenges he made in his pre-trial motions. First, he argues that the district court erred in not dismissing all counts of the indictment for lack of specificity. Second, he argues that the District of Maine was not the proper venue for two of the counts of conviction. Third, he argues that the district court erred in failing to suppress all evidence derived from Yahoo!'s allegedly illegal search of password-protected Yahoo! accounts. Fourth, he argues that the admission of evidence from Yahoo!, Google, and NCMEC violated his Confrontation Clause rights. Finally, he argues that his sentence was erroneous because the district court erred in finding that at least 300 images were involved. We address Cameron's arguments in turn.

A. Sufficiency of the Indictment

Cameron argues that the indictment is insufficient because it fails to identify the specific images that each offense was based on. Federal Rule of Criminal Procedure 7(c)(1) states that an indictment "must be a plain, concise, and definite written statement of the essential facts constituting the offense charged." Fed. R. Crim. P. 7(c)(1). "When grading an indictment's sufficiency, we look to see whether the document sketches out the elements of the crime and the nature of the charge so that the defendant can prepare a defense and plead double jeopardy in any future prosecution for the same offense." United States v. Guerrier, 669 F.3d 1, 3 (1st Cir. 2011). The sufficiency of an indictment is a question of law which we review de novo. Id. (describing question of sufficiency as a "legal issue" to which de novo review applies).

We conclude that the indictment was sufficient. As the district court correctly noted, each count of the indictment included the following information: a description of the offense that tracks the language of the relevant statute, the date of the offense, the type of child pornography involved (digital images), and the means by which Cameron either transported (for example, by uploading to a specified Yahoo! Photos album), received, or possessed the child pornography in question. See Cameron I, 662 F. Supp. 2d at 180-81. Cameron's argument that the indictment is

insufficient because it failed to identify the specific images that each offense was based on is unavailing. As the district court correctly noted, neither the statutes under which Cameron was charged nor Rule 7(c)(1) itself requires such specificity. See id. at 180. Thus, we agree with the district court that the indictment in this case satisfies Fed. R. Crim. P. 7(c)(1)'s requirements.

B. Venue

Cameron argues that venue in Maine was improper for Counts Twelve and Thirteen of the indictment because he was in New York on the dates alleged. Counts Twelve and Thirteen alleged that on August 11, 2007, Cameron transported and received child pornography, respectively, using Google Hello. Cameron argues that since he and his computer were physically located in New York, venue was only proper in New York.

"The right to be tried in the appropriate venue is one of the constitutional protections provided to defendants by the Sixth Amendment." United States v. Scott, 270 F.3d 30, 34 (1st Cir. 2001). As such, "[t]he burden of showing proper venue is on the government, which must do so by a preponderance of the evidence." Id. However, "[w]e review the evidence on venue in the light most favorable to the government." Id. at 35. We review legal conclusions de novo. Id. at 34.

Under 18 U.S.C. § 3237(a) (2012), a crime involving interstate commerce can be "prosecuted in any district from,

through, or into which such commerce, mail matter, or imported object or person moves." Transporting and receiving child pornography via Internet services such as Google Hello are both crimes involving interstate commerce. See id. § 2252A(a)(1) (making it illegal to "transport[]" child pornography "using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer"); id. § 2252A(a)(2)(A) (making it illegal to receive "any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer"). In addition, the district court found from the evidence at trial that the child pornography images Cameron sent and received while in New York were stored on Cameron's Dell Laptop, which he later brought back to Maine. Thus, because the objects of Cameron's commerce moved into the District of Maine, venue there was proper.

We further note that finding venue in Maine is consistent with the purpose of the Constitution's venue protection, which is to "ensure[] that a criminal defendant cannot be tried in a distant, remote, or unfriendly forum solely at the prosecutor's whim." United States v. Salinas, 373 F.3d 161, 164 (1st Cir. 2004). Since Cameron lives in Maine, the District of Maine cannot

be "distant" or "remote" for him, and there is no evidence that the District Court was an "unfriendly" forum.

C. Motion to Suppress

Cameron argues that the district court erred in denying his motion to suppress evidence. He posits that Yahoo!'s search for child pornography in password-protected accounts violated the Fourth Amendment because Yahoo! acted as an agent of the government. Cameron further contends that, because the Yahoo! CP Reports to NCMEC were the result of Yahoo!'s search, and because NCMEC sent CyberTipline Reports to ICAC after receiving Yahoo!'s reports, all subsequent searches executed by ICAC at Cameron's home or executed via search warrants served on Yahoo! and Google derived from Yahoo!'s original illegal searches. Thus, Cameron argues, all evidence obtained as a result of searches conducted during ICAC's investigation should have been suppressed.

In reviewing the denial of a motion to suppress evidence, this court reviews the facts "in the light most favorable to the district court's ruling," and will review any "findings of fact and credibility determinations for clear error." United States v. Camacho, 661 F.3d 718, 723 (1st Cir. 2011) (internal quotation marks and citation omitted). "'A clear error exists only if, after considering all the evidence, we are left with a definite and firm conviction that a mistake has been made.'" Id. (quoting United States v. McCarthy, 77 F.3d 522, 529 (1st Cir. 1996)). "[W]e will

uphold a denial of a motion to suppress if any reasonable view of the evidence supports it." Id. (internal quotation marks and citation omitted). However, "[w]e review de novo the district court's conclusions of law, including its application of the law to the facts." Id. at 724. "The appellant bears the burden of showing a violation of his Fourth Amendment rights." Id.

The Fourth Amendment states that the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. "The Supreme Court has consistently construed the Fourth Amendment protection as limiting only governmental action." United States v. Momoh, 427 F.3d 137, 140 (1st Cir. 2005) (internal quotation marks and citation omitted). The Fourth Amendment does not apply "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." United States v. Jacobsen, 466 U.S. 109, 113 (1984) (emphasis added) (internal quotation marks and citation omitted).

A private search only implicates the Fourth Amendment if the private party acts as a "government agent." Silva, 554 F.3d at 18. In Silva, we established that in determining whether a private party has acted as a government agent, courts must consider three factors: (1) "the extent of the government's role in instigating or

participating in the search"; (2) "[the government's] intent and the degree of control it exercises over the search and the private party"; and (3) "the extent to which the private party aims primarily to help the government or to serve its own interests." Id. (internal quotation marks and citation omitted). We will not find that a private party has acted as an agent of the government "simply because the government has a stake in the outcome of a search." Id.

Here, as to the first Silva factor, there is no evidence that the government had any role in instigating or participating in the search. Yahoo! began searching Cameron's accounts after it received an anonymous tip regarding child pornography in the Yahoo! Photo album of user "lilhottyohh." There is no evidence that the person who sent this tip to Yahoo! was a government employee. Cameron contends that the Yahoo! employees who searched his accounts likely had "strong connections to law enforcement." However, this contention is rank speculation on Cameron's part, with no support in the record.

As to the second Silva factor, there is no evidence that the Government exercised any control over Yahoo! or over the search. As discussed above, Yahoo! employees conducted the search pursuant to Yahoo!'s own internal policy. Furthermore, there is no evidence that the Government compelled Yahoo! in any way to maintain such a policy. Cameron points to the fact that Yahoo had

a duty under federal law to report child pornography to NCMEC in August of 2007. See 42 U.S.C. § 13032(b)(1) (repealed 2008). However, the statute did not impose any obligation to search for child pornography, merely an obligation to report child pornography of which Yahoo! became aware.

Finally, as to the third Silva factor, it is certainly the case that combating child pornography is a government interest. However, this does not mean that Yahoo! cannot voluntarily choose to have the same interest. As discussed above, there is no evidence that the government instigated the search, participated in the search, or coerced Yahoo! to conduct the search. Thus, if Yahoo! chose to implement a policy of searching for child pornography, it presumably did so for its own interests. The record does not reflect what Yahoo!'s interests might have been, but it is Cameron's burden to show that Yahoo! did what it did to further the government's interest, and he can point to no evidence to carry this burden.

Having applied the Silva factors, we conclude that Yahoo! was not acting as an agent of the government; therefore, its searches of Cameron's accounts did not violate the Fourth Amendment. Because there was no Fourth Amendment violation, there was no reason to suppress any evidence that may have derived from Yahoo!'s initial searches. For this reason, we hold that the

district court properly denied Cameron's motion to suppress evidence.

D. Confrontation Clause

Cameron next argues that the district court's admission of evidence obtained from Yahoo!, Google, and NCMEC violated his Confrontation Clause rights. Although Cameron's brief does not make clear which specific records he believes should not have been admitted, he does specify that he is not challenging the admission of those child pornography images that Yahoo provided in response to search warrants. We thus presume that Cameron's challenge is to the following categories of evidence: (1) the Yahoo! Account Management Tool and Login Tracker data -- this data was attached to the CP Reports and was also produced in response to search warrants; (2) electronic receipts of Yahoo's CP Reports to NCMEC -- these receipts were produced by Yahoo! in response to search warrants; (3) NCMEC's CyberTipline Reports to ICAC; and (4) the Google Hello Connection Logs.[7]

---

[7] Cameron makes no coherent challenge to the admission of the emails produced in response to the search warrants served on Yahoo!. Cameron appears to lump these in with the other Yahoo! records. However, as the district court recognized, the emails may be in a legally distinct category from the other records, because they could be viewed as statements attributable to Cameron directly. See Cameron III, 733 F. Supp. 2d at 185 (noting government's argument that "statements attributable to the defendant in the Yahoo! records and emails are not hearsay because a party's own statement is directly admissible against him") (internal quotation marks and citation omitted). Cameron has not explained to this court how any of his Confrontation Clause arguments relate to the emails; for this reason, we deem any

We review de novo a district court's decision that the admission of various exhibits did not violate the Confrontation Clause. See United States v. Mitchell-Hunter, 663 F.3d 45, 49 (1st Cir. 2011).

1. Confrontation Clause Principles

"The Sixth Amendment's Confrontation Clause confers upon the accused in all criminal prosecutions . . . the right . . . to be confronted with the witnesses against him." United States v. Phoeun Lang, 672 F.3d 17, 21 (1st Cir. 2012) (quoting Bullcoming v. New Mexico, 131 S. Ct. 2705, 2713 (2011)) (internal quotation marks omitted). In Crawford, the Supreme Court held that the Confrontation Clause bars the admission of "testimonial statements of witnesses absent from trial," unless the witness is unavailable to testify and the defendant had a prior opportunity for cross-examination. 541 U.S. at 59. Two years later, in Davis v. Washington, the Court held that Crawford's prohibition "applies only to testimonial hearsay." Davis v. Washington, 547 U.S. 813, 823-24 (2006) (emphasis added).[8] Thus, "the threshold question in

---

challenge to the emails waived. See Rodríguez v. Municipality of San Juan, 659 F.3d 168, 175 (1st Cir. 2011) ("[W]e consider waived arguments confusingly constructed and lacking in coherence . . . Judges are not mind-readers, so parties must spell out their issues clearly, highlighting the relevant facts and analyzing on-point authority.") (internal quotation marks and citations omitted).

[8] Hearsay is defined as a statement made out of court, by a person, which is offered into evidence to prove the truth of the matter asserted. Fed. R. Evid. 801(c); United States v. Benítez-Ayala, 570 F.3d 364, 367 (2009).

every case is whether the challenged statement is testimonial. If it is not, the Confrontation Clause has 'no application.'" Figueroa-Cartagena, 612 F.3d at 85 (quoting Whorton v. Bockting, 549 U.S. 406, 420 (2007)).

The Supreme Court has yet to supply a "comprehensive definition of 'testimonial.'" Lang, 672 F.3d at 22 (quoting Crawford, 541 U.S. at 822); see also Davis, 547 U.S. at 822 (deciding narrow issues before the Court "[w]ithout attempting to produce an exhaustive classification of all conceivable statements . . . as either testimonial or nontestimonial"). The Court in Crawford, however, provided an "illustrative list of the 'core class of testimonial statements.'" Lang, 672 F.3d at 22 (quoting Crawford, 541 U.S. at 51). This list included "statements that were made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial." Crawford, 541 U.S. at 52 (internal quotation marks omitted). On the other hand, the Court also indicated that certain types of statements "by their nature [are] not testimonial -- for example, business records or statements in furtherance of a conspiracy," and therefore do not implicate the Confrontation Clause. Crawford, 541 U.S. at 56.

Relying on Crawford, we have held in a number of cases that business records -- or their close counterpart, public records of non-law enforcement government agencies -- are admissible absent

confrontation. See, e.g., Lang, 672 F.3d at 22-23 (holding that an immigration document was not testimonial because an objectively reasonable person would not have understood the form to be used in prosecuting the defendant at trial); United States v. De La Cruz, 514 F.3d 121, 133 (1st Cir. 2008) (concluding that autopsy report was "in the nature of a business record" and thus admissible without confrontation); United States v. García, 452 F.3d 36, 41-42 (1st Cir. 2006) (affirming admission of warrant of deportation in defendant's immigration file).

However, although the Supreme Court seemed to indicate in Crawford that business records are not testimonial "by their nature," 541 U.S. at 56, the Court later indicated that this is not necessarily the case for all business records. In Meléndez-Díaz v. Massachusetts, the prosecutor sought to admit "certificates of analysis" that showed that a substance found in the defendant's possession was cocaine. 557 U.S. 305, 308 (2009). The certificates were sworn to by analysts at a state laboratory. Id. The trial court allowed the certificates, even though the forensic analysts who tested the substance did not testify. Id. at 309. The Supreme Court ruled that the admission of these certificates violated the Confrontation Clause because they fell into the "'core class of testimonial statements'" identified in Crawford. Meléndez-Díaz, 557 U.S. at 310 (quoting Crawford, 541 U.S. at 51). The Court found that the certificates were effectively affidavits,

and that they had clearly been "'made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial.'" Id. (quoting Crawford, 541 U.S. at 52).

In finding that the admission of the certificates violated the Confrontation Clause, the majority rejected the argument that the certificates could be admitted as business records. Although the majority found that the certificates "[did] not qualify as business records," they held that even if the certificates were business records, "their authors would be subject to confrontation nonetheless." Id. at 321. The majority observed that although "[d]ocuments kept in the regular course of business may ordinarily be admitted at trial despite their hearsay status," this would not be so "if the regularly conducted business activity is the production of evidence for use at trial." Id. at 321 (emphasis added). As the majority explained, "[b]usiness and public records are generally admissible absent confrontation not because they qualify under an exception to the hearsay rules, but because -- having been created for the administration of an entity's affairs and not for the purpose of establishing or proving some fact at trial -- they are not testimonial." Id. at 324 (emphasis added). Thus, because the certificates at issue in Meléndez-Díaz had been "prepared specifically for use at petitioner's trial," the court held that "[w]hether or not they

qualif[ied] as business records," they were inadmissible unless their authors could be cross-examined. Id.; cf. Bullcoming, 131 S. Ct. at 2720 ("'[D]ocuments kept in the regular course of business may ordinarily be admitted at trial despite their hearsay status,' except 'if the regularly conducted business activity is the production of evidence for use at trial.' In that circumstance, the hearsay rules bar admission of even business records.") (Sotomayor, J., concurring) (internal citation omitted) (quoting Meléndez-Díaz, 557 U.S. at 321).

Returning to the facts of this case, even if the records at issue here are business records, as the government argues, we must still determine whether or not they are testimonial. See United States v. Pursley, 577 F.3d 1204, 1223 (10th Cir. 2009), cert. denied, ___ U.S. ___, 130 S. Ct. 1098 (2010) ("[E]ven if a statement qualifies for an exception to the hearsay doctrine -- based upon judicially fashioned reliability principles -- the statement's admission may violate the Sixth Amendment's mandate for 'confrontation' if it constitutes 'testimonial' hearsay." (citing Crawford, 541 U.S. at 61-62; Meléndez-Díaz, 129 S. Ct. at 2533)). "To rank as 'testimonial,' a statement must have a 'primary purpose' of 'establishing or proving past events potentially relevant to later criminal prosecution.'" Bullcoming, 131 S. Ct. at 2714 n.6 (quoting Davis, 547 U.S. at 822). "In identifying the primary purpose of an out-of-court statement, we

apply an objective test." Williams v. Illinois, 132 S. Ct. 2221, 2243 (2012) (plurality opinion).

With these principles in mind, we proceed to determine whether the records Cameron challenges are testimonial in nature.

2. Yahoo! Account Management Tool, Yahoo! Login Tracker, and Google Hello Connection Logs

It is clear that the admission of the Yahoo! Account Management Tool data, the Yahoo! Login Tracker data, and the Google Hello Connection Logs did not violate the Confrontation Clause. Lee, the Yahoo! witness, testified that all of the data in the Account Management Tool and the Login Tracker was data that Yahoo! collected automatically in order to further its business purposes. Bogart, the Google witness, testified in a similar fashion regarding the Google Hello Connection Logs. Although "Crawford analysis generally requires a court to consider two threshold issues: (1) whether the out-of-court statement was hearsay, and (2) whether the out-of-court statement was testimonial," United States v. Earle, 488 F.3d 537, 542 (1st Cir. 2007), we dispense with the first issue because, even assuming arguendo that the documents in question contain hearsay statements, the same are in no way testimonial. As the government argues, these documents squarely conform to the requirements outlined by the Federal Rules of Evidence for business records: (1) they were made at or near the time of the event; (2) kept in the regular course of business; and (3) created in the regular course of business. See Fed. R. Evid.

803(6).[9] Thus, we agree with the government that the Account Management Tools and the Login tracker were business records of Yahoo!, and the Google Hello Connection Logs were business records of Google.[10]

---

[9] Rule 803(6) provides that "[a] record of an act, event, condition, opinion, or diagnosis" is admissible despite its hearsay status if:

> (A) the record was made at or near the time by -- or from information transmitted by -- someone with knowledge;
> (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;
> (C) making of the record was a regular practice of that activity;
> (D) all these conditions are shown by the testimony of the custodian or another qualified witness . . .; and
> (E) neither the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.

[10] Rule 803(6) also requires that the records be introduced through the testimony of a "custodian or other qualified witness," and that neither the "source of information nor the method or circumstances of preparation" can "indicate a lack of trustworthiness." Cameron protests that Lee and Bogart were not engineers, had no knowledge of the technical details of Yahoo!'s or Google's systems, respectively, and were not the ones who prepared the records. However, when dealing with computerized records under Rule 803(6), "it is not required that the qualified witness be a computer programmer . . . or that she be the person who actually prepared the record." United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991) (internal quotation marks and citation omitted). The rule simply requires that the witness be "one who can explain and be cross-examined concerning the manner in which the records are made and kept," Wallace Motor Sales v. American Motors Sales Corp., 780 F.2d 1049, 1061 (1st Cir. 1985), and Lee and Bogart satisfied this requirement. As for the trustworthiness of the records, we have held that "the ordinary business circumstances described [by the qualified witness] suggest trustworthiness at least where absolutely nothing in the record in any way implies lack thereof." Moore, 923 F.2d at 915 (internal citation omitted). Such is the case here, since there is no evidence in the record that Yahoo!'s

Moreover, it is clear that none of these records are the type of "testimonial" business records that might cause Confrontation Clause concerns under Meléndez-Díaz. Lee testified that Yahoo! kept the Account Management Tool and Login Tracker data in order to serve business functions that were totally unrelated to any trial or law enforcement purpose: namely, to provide reliable data about its customer accounts. Bogart provided similar testimony regarding Google's need for the Google Hello Connection Logs. Thus, applying an "objective test," Williams, 132 S. Ct. at 2243, we find that the "primary purpose" of collecting this data was not to "establish[] or prov[e] past events potentially relevant to later criminal prosecution." Bullcoming, 131 S. Ct. at 2714 n.6. We therefore conclude that the district court did not err in admitting the Yahoo! Account Management Tool evidence, the Yahoo! Login Tracker evidence, or the Google Hello Connection Logs evidence.

3. Receipts of Yahoo! CP Reports

We are not convinced that the same can be said for the receipts of the Yahoo! CP Reports. As Lee testified, Yahoo! created CP Reports in the ordinary course of its business. Yahoo! also kept receipts of those Reports, which were essentially copies of the Reports, in the ordinary course of its business. Thus, in analyzing whether the receipts of the CP Reports are testimonial,

---

or Google's data recording systems were flawed in any way.

we consider whether the CP Reports themselves -- of which the receipts are simply computer-generated copies -- are (1) out-of-court hearsay statements, and (2) whether these statements are testimonial. Earle, 488 F.3d at 542.

In order to constitute hearsay, the CP Reports must be: (1) statements made out of court, (2) by a person, and (3) offered into evidence to prove the truth of the matter asserted. Fed. R. Evid. 801(b) and (c). As to the first prong, we have no trouble finding that the CP Reports are out-of-court statements, as they are written assertions, made outside of the courtroom, containing information on screen names that Yahoo! has associated with potential child pornography. We also find that the second prong is met as the CP Reports were made by a person, as Lee himself testified that they were made by a person with knowledge of their contents. According to Lee, someone at Yahoo!'s Legal Department reviews an archive of the images featured in the suspect's account, removes those that do not appear to contain child pornography, and includes the rest in the CP Report addressed to NCMEC. Although the receipts of the CP Reports in question do not appear to be signed by any Yahoo! employee in particular, we believe it to be evident from Lee's testimony that the CP Reports were authored by an employee in the Legal Department. Lee himself testified that part of his duties at Yahoo! included preparing these CP Reports. Therefore, the CP Reports as a whole are statements made by a

person, who intended those statements to be taken as true, and subsequently acted on, by NCMEC. As we will explain infra, this is the case despite the fact that some of the information contained in the CP Reports was generated automatically by Yahoo!'s different retrieval tools.

Lastly, we conclude that the receipts of the CP Reports were introduced at trial to prove the truth of at least some of the matters asserted in them. The government sought to introduce this evidence to establish a link between the "Suspect IP Address" contained in the CP Reports and Cameron. The prosecution was seemingly operating under the impression that this IP address was the one from which the most recent image of child pornography had been uploaded, even though, as previously explained, this association is not readily apparent from the documents themselves. Consequently, we can only infer that it was the government's intent to use this evidence to link Cameron to the specific IP addresses from which child pornography images were uploaded into the Yahoo! accounts, and not just to support the proposition that said IP addresses were the ones from which Cameron registered the accounts at Yahoo!. To establish the latter, the government could have simply relied on the Yahoo! Account Management Tool, the admission of which we have just held did not implicate the Confrontation Clause.

The district court apparently went along with this characterization of the CP reports when it decided to admit their receipts into evidence. In doing so, the court went through a three-step logical sequence aimed at ultimately linking Cameron to the IP addresses and the Yahoo! screen names used to upload the images, just as the government had proposed. First, the district court used the receipts of the CP Reports to link the Yahoo! screen names to the IP addresses from which the suspect images were uploaded. Second, the district court used the NCMEC CyberTipline Reports to make the connection between these IP addresses and the crime of uploading child pornography images, by examining the images attached to these reports and making a preliminary finding that they portrayed child pornography as defined in federal law.[11] Lastly, the court found that the incriminating IP addresses were linked to Cameron based on the evidence obtained from sources such as "eBay", "PayPal" and the "Military Watch Forum" website, which evinced that Cameron had used those same IP addresses to log in to his personal accounts with those entities during the same time periods that the uploads took place. From this we can soundly conclude that the receipts of the Yahoo! CP Reports were introduced as identifying evidence, designed to unveil Cameron as the person responsible for uploading child pornography using the Yahoo! screen

[11] It should be noted that the receipts of the Yahoo! CP Reports introduced into evidence did not contain any actual images of child pornography, unlike the NCMEC CyberTipline Reports, which did.

names featured in some of the counts of the indictment. Hence, these receipts were introduced to prove the truth of the matter asserted and as such constitute hearsay.

The next step in our inquiry calls upon us to determine whether the receipts of the CP Reports are testimonial. We assume that the CP Reports, and by extension the receipts, would count as business records for the purposes of Federal Rule of Evidence 803(6). However, unlike the Yahoo! Account Management Tool, the Login Tracker data and the Google Hello Connection Logs, there is strong evidence that the CP Reports were prepared with the "primary purpose of establishing or proving past events potentially relevant to a later criminal prosecution." Bullcoming, 131 S. Ct. at 2714 n.6 (internal quotation marks and citation omitted). We also find that the Reports are similar in purpose to the types of out-of-court statements that the Supreme Court has described as testimonial in recent Confrontation Clause cases. See Davis, 547 U.S. at 828-29 (statements to law enforcement in non-emergency situation); Meléndez-Díaz, 557 U.S. at 321 (documents created in the ordinary course of business but also for litigation purpose). Thus, although the CP Reports may have been created in the ordinary course of Yahoo!'s business, they were also testimonial; the receipts of the Reports, therefore, should not have been admitted without giving Cameron the opportunity to cross-examine the Yahoo! employees who prepared the CP Reports.

We start by objectively viewing the evidence to determine the "primary purpose" of the Reports. Firstly, we note that the CP Reports refer to a "Suspect Screen Name," a "Suspect Email Address," and a "Suspect IP Address." A "suspect" is "one who is suspected; esp. one suspected of a crime or of being infected." Webster's Third New International Dictionary 2303 (2002). There was no testimony from Lee, nor any other evidence, that Yahoo! treated its customers as "suspects" in the ordinary course of its business. Indeed, the word "suspect" does not appear anywhere in the Account Management Tool or Login Tracker data. Further, Lee testified that in order for a CP Report to initially have been created, someone in the Legal Department had to have determined that an account contained what appeared to be child pornography images.

Secondly, once Yahoo! created a CP Report, it did not merely keep it in its own files; rather, it sent the report on to NCMEC (and kept a receipt). Although NCMEC is not officially a government entity, it receives a grant from the government, and one of the uses to which NCMEC puts this grant money is to operate the CyberTipline and forward reports of child pornography to law enforcement. See 42 U.S.C. § 5773(b)(1)(P).

Given that Yahoo! created CP Reports referring to "Suspect[s]" and sent them to an organization that is given a government grant to forward any such reports to law enforcement, it

is clear that under the "objective test" required by Williams, 132 S. Ct. at 2243, the primary purpose of the CP Reports was to "establish[] or prov[e] past events potentially relevant to later criminal prosecution." Bullcoming, 131 S. Ct. at 2714 n.6 (internal quotation marks and citation omitted). The reports clearly "established past events," in that each one reflected the "event" of child pornography being placed into a Yahoo! user account at some point in the past. These "events" were clearly "relevant to later criminal prosecution": uploading child pornography and possessing it on the Internet are crimes, and evidence as to the IP address, and screen name of the suspect, is clearly relevant to prosecuting those crimes. We also find that the CP Reports were "made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial." Crawford, 541 U.S. at 52 (internal quotation marks and citation omitted). Lee testified that it was Yahoo!'s standard practice to send CP Reports to NCMEC and keep receipts of those Reports; thus, whoever generated the CP Reports in this case presumably knew that the Reports would most likely spark an investigation, and that as a result of such investigation, the government might request the CP Reports (in the form of the receipts) from Yahoo! for use as evidence.

Our conclusion is bolstered by a comparison of the CP Reports at issue here with those statements the Supreme Court has

found to be testimonial or non-testimonial in recent Confrontation Clause cases. For example, the CP Reports here are similar in many ways to those statements that the Supreme Court found to be testimonial in Davis. Davis concerned two consolidated cases. 547 U.S. at 817. In the first case, the former girlfriend of Adrian Davis ("Davis") called 911 to report that Davis was assaulting her, and narrated Davis's attack to the operator as it occurred. Id. at 817-18. At Davis's trial, the girlfriend did not testify, but the court admitted the recording of the 911 call, and Davis was convicted of violation of a domestic no-contact order. Id. at 818-19. In the second case, the police responded to a domestic disturbance at the home of Hershel Hammon ("Hammon"). Id. at 819. The police separately questioned Hammon and his wife, the latter of whom swore out an affidavit stating that Hammon had attacked her. Id. at 820. Hammon's wife did not testify at his trial, but the court introduced her affidavit, and Hammon was found guilty. Id. at 820-21.

In Davis's case, the Court found that the recording was not testimonial because the primary purpose of Davis's girlfriend's statements to the 911 operator were "to enable police assistance to meet an ongoing emergency." Id. at 828; see also id. at 827 ("A 911 call . . ., and at least the initial interrogation conducted in connection with a 911 call, is ordinarily not designed primarily to establish or prove some past fact, but to describe current

circumstances requiring police assistance.") (internal quotation marks omitted). However, in Hammon's case, the Court found that his wife's affidavit was testimonial, because "[i]t [was] entirely clear from the circumstances that the interrogation was part of an investigation into possibly criminal past conduct." Id. at 829.

Here, the CP Reports are more similar in purpose to Hammon's wife's affidavit than to the recording of Davis's girlfriend's 911 call. The CP Reports were clearly not intended "to enable police assistance to meet an ongoing emergency" or to "describe current circumstances requiring police assistance." Davis, 547 U.S. at 827-28. While possession of child pornography is a serious crime, and while discovering child pornography must certainly have troubled Yahoo! and its employees, the presence of child pornography in Cameron's accounts was certainly not an "emergency" comparable to what Davis's girlfriend described to the 911 operator: an ongoing physical assault. Cf. Michigan v. Bryant, 131 S. Ct. 1143, 1166-67 (2011) (holding that statements by gunshot victim to police identifying the shooter were not testimonial when police had reason to believe that the shooter might still be armed and in the area). Rather, the CP Reports were clearly intended to lead to "an investigation into possibly criminal past conduct." See Davis, 547 U.S. at 829. And although the Court in Davis found it "unnecessary to consider whether and when statements made to someone other than law enforcement personnel are 'testimonial,'"

Davis, 547 U.S. at 823 n.2, we find that in the context of this case, NCMEC effectively acted as an agent of law enforcement, because it received a government grant to accept reports of child pornography and forward them along to law enforcement. Cf. id. ("If 911 operators are not themselves law enforcement officers, they may at least be agents of law enforcement when they conduct interrogations of 911 callers. For the purposes of this opinion . . . we consider their acts to be that of the police.").

We recognize that both cases in Davis involved "interrogations," see id. at 822 n.1, and that the CP Reports here did not result from any "interrogation" of Yahoo!. However, as noted above, Yahoo! was obligated under federal law to report any child pornography it became aware of to NCMEC. See 42 U.S.C. § 13032(b)(1) (current version at 18 U.S.C. § 2258A(a)(1)). Moreover, the Court in Davis noted that although the decision referred to "interrogations," "[t]his [was] not to imply ... that statements made in the absence of any interrogation are necessarily nontestimonial." Davis, 547 U.S. at 822 n.1. "The Framers," the Court noted, "were no more willing to exempt from cross-examination volunteered testimony or answers to open-ended questions than they were to exempt answers to detailed interrogation." Id. (emphasis added). The CP Reports at issue here, we conclude, fall somewhere in the range between "volunteered testimony" and responses to an interrogation, and we are confident that the Framers would not have

been willing to exempt testimonial statements in this range from cross-examination.

The situation here is also similar to that in Palmer v. Hoffman, 318 U.S. 109 (1943), which the Court in Meléndez-Díaz cited as an example of a case where the "regularly conducted business activity [was] the production of evidence for use at trial." 557 U.S. at 321 (citing Palmer, 318 U.S. 109). Palmer involved an accident at a railroad crossing in Massachusetts. 318 U.S. at 110. The train's engineer, who died before trial, gave a statement about the accident to a railroad official and to a representative of the Massachusetts Public Utilities Commission. Id. at 111. The railroad sought to introduce the engineer's statement under the Act of June 20, 1936, 49 Stat. 1561 (current version, as amended, at 28 U.S.C. § 1732 (2012)), which allowed the admission in federal court of any "memorandum or record of any act, transaction, occurrence, or event" as long as such record "was made in the regular course of any business." Palmer, 318 U.S. at 111, 111 n. 1. The Supreme Court held that the record was properly excluded, noting that the statement was not "a record made for the systematic conduct of the business as a business," but rather was "calculated for use essentially in the court, not in the business." Id. at 113, 114; see also Meléndez-Díaz, 557 U.S. at 321 (explaining the holding of Palmer). Here, the fact that the CP Reports were made pursuant to a standard Yahoo! business practice

does not mean they were made to advance Yahoo!'s core business purpose, which is, as Lee testified, to offer Internet-based services such as e-mail, search, and instant messaging. Just as the "primary utility" of the report in Palmer was "in litigating, not in railroading," 318 U.S. at 114, the primary utility of the CP Reports here is in reporting crimes to law enforcement, not in providing Internet-based services to Yahoo!'s customers.

Finally, we believe the CP Reports here are distinguishable from the out-of-court statements that a plurality of the Justices found to be non-testimonial in Williams, the Supreme Court's most recent Confrontation Clause case. In Williams, vaginal swabs from a sexual-assault kit were sent to Cellmark Diagnostics Laboratory ("Cellmark"), which produced a DNA profile from the semen found in the swabs. 132 S. Ct. at 2229 (Alito, J., plurality opinion). At Williams's trial, the prosecution called as a witness Sandra Lambatos ("Lambatos"), an expert in biology and DNA analysis. Id. Lambatos testified that the DNA profile produced by Cellmark matched the DNA profile of Williams, which was already in a state database as a result of a prior unrelated arrest. Id. Although the Cellmark report was not admitted into evidence at all, the Williams plurality held that "[e]ven if the Cellmark report had been introduced for its truth, we would nevertheless conclude that there was no Confrontation Clause violation." Id. at 2242.

Based on the circumstances of the case, the plurality concluded that "the primary purpose" of the Cellmark report, "viewed objectively, was not to accuse [Williams] or create evidence for use at trial." Id. at 2243. The plurality noted that when the state sent the kit to Cellmark, the state's "primary purpose was to catch a dangerous rapist who was still at large, not to obtain evidence for use against [Williams], who was neither in custody nor under suspicion at the time." Id. The plurality also noted that "no one at Cellmark could have possibly known that the profile it produced would turn out to inculpate [Williams] -- or for that matter, anyone else whose DNA profile was in a law enforcement database." Id. at 2243-44. The plurality further noted that in DNA labs, "the technicians who prepare a DNA profile generally have no way of knowing whether it will turn out to be incriminating or exonerating -- or both." Id. at 2244.

This last point is critical in distinguishing the Cellmark reports in Williams from the Yahoo! CP Reports here. Nobody at Yahoo! who was involved in creating the CP Reports could possibly have believed that the CP Reports could be other than "incriminating." Recall that (1) Yahoo! created these Reports after its own employees had already concluded that a crime had been committed, and (2) Yahoo! then sent these Reports to an organization that forwards such reports to law enforcement. Yahoo!'s employees may not have known whom a given CP Report might

incriminate, but they almost certainly were aware that a Report would incriminate somebody.

The government contends that we should focus not on the purpose for which the CP Reports were created, but rather on the purpose for which the records underlying the CP Reports -- such as the record of the user's IP address, and the associations between images and accounts -- were created. Because these underlying records were created for a Yahoo! core business purpose, the government contends that under the "primary purpose" test, the CP Reports are not testimonial. The government urges us to treat the Yahoo! CP Reports like the immigration documents we held to be non-testimonial in Lang, 672 F.3d at 22-23, or like the types of business records that other Circuits have found to be non-testimonial. See, e.g., United States v. Yeley-Davis, 632 F.3d 673, 677-81 (10th Cir. 2011) (holding that neither cell phone records nor their authenticating documents were testimonial); United States v. Ali, 616 F.3d 745, 751-52 (8th Cir. 2010) (holding that bank records regarding taxpayer refund anticipation checks were not testimonial).

However, the government's argument ignores a critical point: as explained earlier, the CP Reports are themselves "statements," and thus their purpose must be analyzed independently. It is not enough to analyze the purpose behind the creation of the business records on which the CP Reports rely. If

the CP Reports simply consisted of the raw underlying records, or perhaps underlying records arranged and formatted in a readable way for presentation purposes, the Reports might well have been admissible. See Lang, 627 F.3d at 22-23; Yeley-Davis, 632 F.3d at 677. Indeed, we have upheld the admission of the Account Management Tool and Login Tracker printouts because those exhibits simply take pre-existing records (records such as the IP addresses from which an account was created and accessed) and put them on paper in a readable format. But the CP Reports are a different animal, for they do not merely present pre-existing data; instead, they convey an analysis that was performed using pre-existing data.

From our earlier discussion, recall that the CP Reports and Lee's testimony clearly indicated that, to create each Report, someone at Yahoo! analyzed Yahoo!'s data, drew conclusions from that data, and then made an entirely new statement reflecting those conclusions. Each report also refers to a "Suspect" who is identified by his "Screen Name," "Email Address," "IP Address," and "URL." This means that someone at Yahoo! analyzed Yahoo!'s business records and concluded that (1) a crime had likely been committed and (2) a particular user likely committed that crime.[12] Thus, every Yahoo! CP Report was a new statement that conveyed an

[12] We do not treat the pictures themselves as business records of Yahoo!. However, the association between a picture and an account is clearly a business record of Yahoo!; without keeping track of these associations, Yahoo! could not figure out which photos on its servers belonged to which users.

analysis that had not existed previously. The new statement was, in effect, "someone has committed a crime, here is the evidence that a crime was committed, and here is how to identify the perpetrator." The primary purpose of this new statement was law enforcement-related, even if the primary purpose of the data used to support the statement was not. Our conclusion here is strengthened by the fact that in preparing the CP Reports, the Yahoo! employees removed the images they thought did not depict child pornography, as said images would presumably not be relevant to the prosecution of a child pornography crime.

The fact that Yahoo! attached to each CP Report the records that justified its analysis -- the Account Management Tool, Login Tracker, and Image Upload Data -- does not mean that the CP Report itself was not a new statement. By creating the CP Report, the author of the report went beyond simply furnishing pre-existing records and crossed the line into testifying regarding the meaning of those records; in this circumstance, Cameron had the right to confront the author. Cf. Meléndez-Díaz, 557 U.S. at 322 (noting that traditionally, a clerk was allowed to "'certify to the correctness of an [official] record kept in his office,' but had 'no authority to furnish, as evidence for the trial of a lawsuit, his interpretation of what the record contains or shows, or to certify to its substance or effect'") (quoting State v. Wilson, 75 So. 95, 97 (La. 1917)). Indeed, the distinction between business

records and statements about those records was recognized by the Eighth Circuit in Ali, a case on which the government relies. In Ali, the prosecution introduced "exhibit 95," which consisted of two parts: (1) records from a bank, HSBC, regarding three taxpayers' refund anticipation checks; and (2) a letter from a manager at HSBC that explained the meaning of the records. 616 F.3d at 751. The HSBC manager wrote that the letter was a "written statement to verify that [the three taxpayers] filed 2002 income tax returns with Cedar Tax Services and applied for Refund Anticipation Checks." Id. The Eighth Circuit held that while the bank records were nontestimonial, "[t]he letter was arguably equivalent to live, in-court testimony and thus not admissible as a business record." Id. at 752.[13]

---

[13] At oral argument, the government analogized Yahoo! to a bank that records statements of financial transactions. The government contended that if the bank detected suspicious activity in certain statements, and if the bank collected those statements and reported those transactions to the authorities, the bank's financial transaction statements would not become testimonial simply because the bank aggregated them in order to make its report. In support of this proposition, the Government relied on United States v. Naranjo, 634 F.3d 1198 (11th Cir. 2011).

However, the government's analogy is inapplicable to the analysis of the CP Reports. The bank records in the government's example are the equivalent to the Account Management Tool, Login Tracker, or Image Upload Data in this case. These documents, like the bank records in the government's example, did not become testimonial simply because they turned out to be relevant to a prosecution. The CP Reports, however, have no equivalent in the government's example. The Reports are documents that contain analyses based on certain other records that were performed only after criminal activity was detected.

It may be the case that the new statement represented in each CP Report -- "someone has committed a crime, here is the evidence that a crime was committed, and here is how to identify the perpetrator" -- was an obvious conclusion based on the underlying data. Presumably any Yahoo! employee who saw child pornography images in a user's account would conclude that the user is at least a "suspect" in a child pornography crime, and that the "suspect's" IP address is the one associated with that account. But one small analytical step for man can sometimes be one giant leap for Confrontation Clause purposes. To hold that the CP Reports are admissible without confrontation as business records simply because they state obvious conclusions based on data in other business records would be to "return to [the Supreme Court's] over-ruled decision in [Ohio v. Roberts], which held that evidence with 'particularized guarantees of trustworthiness' was admissible

---

In addition, Naranjo is of limited relevance to this case because it is clearly distinguishable on its facts. In Naranjo, the Eleventh Circuit held that bank records and checks could be admitted into evidence as non-testimonial business records. 634 F.3d at 1213-14. However, the defendant's Confrontation Clause argument on appeal was aimed not at these records, but on summary charts based on the records that were prepared by a government agent. The Eleventh Circuit held that the charts were admissible because they simply summarized underlying data that was non-testimonial. Id. at 1213. However, the defendant was able to cross-examine the agent who prepared the summary charts, and the district court had instructed the jury to refer to the charts "only as an aid . . . and not for the truth." Id. (internal quotation marks omitted). Here, Cameron had no opportunity to cross-examine the author of the CP Reports. Moreover, we deem the CP Reports to be more than a mere "summary" of other data; rather, they are an analysis of other data.

notwithstanding the Confrontation Clause." Meléndez-Díaz, 557 U.S. at 317 (quoting Ohio v. Roberts, 448 U.S. 56, 66 (1980)). See also Crawford, 541 U.S. at 62 ("Dispensing with confrontation because testimony is obviously reliable is akin to dispensing with jury trial because a defendant is obviously guilty. This is not what the Sixth Amendment prescribes.").

Because the CP Reports were testimonial, the receipts stored by Yahoo! were necessarily testimonial as well. Thus, they should not have been admitted without giving Cameron the opportunity to cross-examine the Yahoo! employees who prepared the CP Reports. We therefore conclude that the admission of the receipts in this case violated Cameron's rights under the Confrontation Clause.

4. CyberTipline Reports

Cameron also assails the admission of the NCMEC CyberTipline Reports, arguing further violations of his rights under the Confrontation Clause. The government's response is that the CyberTipline Reports are not actually "statements" of NCMEC, because NCMEC merely forwards Yahoo!'s CP Reports to the appropriate law enforcement agency. We conclude, however, that this argument is unavailing, as we have already determined that the Yahoo! CP Reports from which the CyberTipline Reports are derived are testimonial. By the government's logic, NCMEC would simply be forwarding testimonial statements made by Yahoo! to law

enforcement. Therefore, the Confrontation Clause problems we find with the admission of CP Reports taint the admission of the CyberTipline Reports.

In any event, we are not convinced that the record supports the government's contention that the CyberTipline Reports "contain exactly the same information present in" the Yahoo! CP Reports. In fact, we believe the record supports an opposite reading, which is that NCMEC does not always send along exactly what it receives from Yahoo! to law enforcement. Our analysis below supports the conclusion that these reports were new statements made by NCMEC and constituted testimonial hearsay statements which were admitted into evidence in violation of Cameron's Confrontation Clause rights.

First, the CyberTipline Reports were introduced into evidence to prove the truth of the matters asserted in them. Our previous discussion outlining the district court's reasoning in admitting the Yahoo! CP Reports demonstrates that the CyberTipline Reports were admitted as part of a batch of evidence aimed at proving that Cameron had uploaded child pornography images onto several Yahoo! accounts. In fact, without the CyberTipline Reports the prosecution would not have been able to prove Cameron's guilt as to Counts One, Two, Three, Four, Five, Eleven and Fourteen of the Indictment, which exclusively charge Cameron with uploading digital images of child pornography onto specific Yahoo! accounts

on specific dates. The only piece of evidence the government could have relied on to establish the specific dates on which Cameron had uploaded the offending images was the CyberTipline Reports, which reflected the date and time on which the most recent image of child pornography had been uploaded, as well as the IP address from which that upload had originated.[14]

The receipts of the Yahoo! CP Reports alone were not enough to sustain Cameron's convictions under the above-referenced counts because they did not contain the specific date of each upload, nor did they contain the actual images that were uploaded. As mentioned earlier, a list of the IP Addresses from which each of the images were uploaded, along with the date and time of each

[14] For example, Count Eleven charged Cameron with uploading child pornography images to the "lilhottee00000" account on July 26, 2007. The evidence from Time Warner and other sources showed that Cameron's residence had been assigned the IP address 76.179.26.185 on that date. To show that child pornography was uploaded to the "lilhottee00000" account on that date, the government pointed to a CyberTipline Report for "lilhottee00000." This Report indicated that the "most recent file or image upload available" in the data sent from Yahoo! was uploaded from 76.179.26.185, and further indicated that the "upload date" was July 26, 2007 at 9:37 AM Pacific Daylight Time. We have found no other exhibit in the record that indicates that child pornography was uploaded to the "lilhottee00000" account on July 26, 2007. Nor is there any other exhibit that shows that child pornography was uploaded to this account from IP address 76.179.26.185. The CP Report that Yahoo! sent to NCMEC for "lilhottee00000" does not show the times at which images were uploaded or the IP addresses from which they were uploaded (the report shows a "Suspect IP Address" of 76.179.26.185, which is the IP address Yahoo! "associated" with the account, but Lee did not explain how the address was "associated"). The Image Upload Data attached to the CP Report had this information, according to Lee, but the government does not appear to have introduced this data into evidence.

upload, was contained in the Image Upload Data that Yahoo! sent to NCMEC as part of each CP Report. However, from our review, it does not appear that this data was included with the CP Report receipts the prosecution introduced at trial, or anywhere else on the record for that matter. Therefore, the CyberTipline Reports were introduced -- and admitted -- into evidence to prove the truth of the assertions contained therein, most importantly: that child pornography images were uploaded onto a particular Yahoo! account, and that the most recent one of those images was uploaded from a specific IP Address on a specific date and time.

The reasoning above defeats the government's argument that the CyberTipline Reports are not really "statements" of NCMEC because all they do is simply convey information sent to NCMEC by companies like Yahoo! to law enforcement. The government relies on testimony from Shehan, the NCMEC witness, to the effect that NCMEC does not add anything to the reports it receives via the CyberTipline, aside from a "report ID" number and an "entry date" for the report. However, this does not explain the fact that the CyberTipline Reports reflect the date and time of the most recent child pornography image upload, while the receipts of the Yahoo! CP Reports do not. As mentioned earlier, the only reasonable explanation we can surmise is that the NCMEC employee who created these reports analyzed the information contained in the Image Upload Data sent by Yahoo!, picked the IP Address from which the

most recent image was uploaded, and included this information, along with the date and time of that upload, in the CyberTipline Report. We note that the Yahoo! CP Reports did not specify whether the "Suspect IP Address" was the IP Address from which the most recent image of child pornography had been uploaded, a representation which was in fact made in the CyberTipline Reports. Therefore, in order to make this representation, the NCMEC employee who prepared the CyberTipline Reports had to have analyzed the Image Upload Data sent by Yahoo!.

In doing so, the NCMEC employee undertook a similar exercise to the one performed by the Yahoo! employee who created the CP Reports; they both analyzed the underlying information in the Image Upload Data and then used that information to create a separate, independent statement. The new statement made by NCMEC can be characterized along these lines: "based on the Yahoo! data, we have determined that the IP Address used by the suspect to upload the most recent image of child pornography is X, and the date and time of this upload is Y and Z."

Having determined that the CyberTipline Reports were indeed new statements by NCMEC, the question now is whether they were testimonial. The answer must be "yes," for it is clear that the "primary purpose" of a CyberTipline Report is to "establish[] or prov[e] past events potentially relevant to later criminal prosecution." Bullcoming, 131 S. Ct. at 2714 n.6 (internal

quotation marks and citation omitted). Indeed, Shehan conceded as much during cross-examination:

> Q: "Mr. Shehan, the sole purpose of the reports that are embodied by Exhibits . . . 10A through 10M [the CyberTipline Reports] is to prove facts at trial, correct?"
>
> A: "It's to be part of the record, yes."

In addition, the primary purpose is also reflected on the face of the reports themselves, which state: "Law enforcement officials please be advised: this Report is being provided solely for the purpose of a law enforcement investigation into possible criminal behavior." (emphasis on original removed).

Even without the above, we would have no trouble finding that the CyberTipline Reports were testimonial. As such, they could not have been admitted without giving Cameron the opportunity to cross-examine their authors. Shehan admitted that he was "not the original analyst who processed" the Yahoo! CP Reports in this case. Thus, the admission of the CyberTipline Reports in these circumstances violated the Confrontation Clause.

E. Harmless Error Analysis

That certain evidence was admitted in violation of Cameron's Confrontation Clause rights does not necessarily mean that we must reverse Cameron's convictions on any counts. Instead, we must determine whether or not the error was harmless beyond a reasonable doubt; if the error was harmless, we will not reverse. See United States v. Meises, 645 F.3d 5, 24 n.26 (1st Cir. 2011)

("Constitutional errors, such as a Confrontation Clause violation, require reversal unless shown to be harmless beyond a reasonable doubt." (emphasis added) (citing United States v. Cabrera-Rivera, 583 F.3d 26, 36 (1st Cir. 2009))). In Cabrera-Rivera, we explained that

> [i]n evaluating harmlessness, we consider a number of factors, including whether the challenged statements were central to the prosecution's case; whether the statements were merely cumulative of other (properly admitted) evidence; the strength of corroborating or contradicting evidence; the extent to which cross-examination was permitted; and the overall strength of the case.

583 F.3d at 36 (citing Earle, 488 F.3d at 546). The burden of proving harmlessness is on the government. Earle, 488 F.3d at 545 (referring to "[the government's] burden of showing that any such error was harmless beyond a reasonable doubt").

It is clear that for many of the counts of conviction, the CP Report receipts and CyberTipline Reports were not even relevant, much less "central," to the prosecution's case. Cameron's guilt on the five counts related to Google Hello -- counts Six, Seven, Nine, Twelve, and Thirteen -- was provable beyond a reasonable doubt using the Google Hello Connection Logs, which were properly admitted. Likewise, Cameron's Yahoo! email and the child pornography found on his computer showed beyond a reasonable doubt that he received child pornography via email as charged in Count Ten. Finally, Cameron's guilt on Count Fifteen,

the child pornography possession count, was proven using the child pornography images found on his computer. Cameron argues that "spillover" prejudice from the improperly admitted records taints these convictions as well, but this argument is meritless. Cameron's trial was a bench trial, and we are confident that the district court was capable of recognizing which evidence was relevant for each count of conviction. Cf. United States v. Zayas, 876 F.2d 1057, 1059 (1st Cir. 1989) (in the context of bench trial, holding that "spillover effect . . . was minimal").

However, for those counts that were based solely on Cameron's alleged uploading of child pornography images to Yahoo! accounts -- counts One, Three, Four, Five, Eleven, and Fourteen -- we conclude that the admission of the Yahoo! CP Reports and the CyberTipline Reports was not harmless. As we have explained, in those counts the government charged Cameron with very specific conduct: uploading child pornography to specified Yahoo! Photo accounts on specified dates. The government was able to establish which IP addresses Cameron had on the dates in question through evidence from Time Warner and other companies. But to prove that Cameron actually uploaded child pornography to the accounts in question on the dates in question, the government needed to introduce evidence showing that (1) child pornography had been uploaded to those accounts on the specific dates in question from the same IP addresses that Cameron had on those dates; and (2) no

one else in Cameron's household but Cameron himself could have been the one who uploaded the images. And again, as far as we can tell from the record, the only evidence that was introduced to demonstrate the upload dates and the upload IP addresses was the CyberTipline Reports. Thus, the improperly admitted reports were "central to the prosecution's case" and were not "cumulative of other (properly admitted) evidence." Cabrera-Rivera, 583 F.3d at 36.[15]

Our result might be different if the government could point us to other admitted evidence specifically showing (1) that child pornography had been uploaded to the accounts identified in the indictment (2) on the dates specified in the indictment (3) from the IP addresses that Cameron had on those dates. For example, the government might have introduced the Image Upload Data from Yahoo!; the government presumably could have acquired this data, as Lee testified that Yahoo! stored it with the receipts. However, it is not clear from the trial transcript or the parties' briefs whether Yahoo! in fact produced this to the government; and in any case, it appears the government did not attempt to introduce it at trial. Since it is the government's burden to prove harmlessness, and since we find no indication that any alternate

[15] Cameron does not challenge the government's showing that neither his wife nor his children could have been the ones who uploaded the images.

evidence was actually admitted, we must reverse Cameron's convictions for Counts One, Three, Four, Five, and Eleven.[16]

F. Sentencing Challenge

Because we must reverse Cameron's conviction with respect to six counts, we need not reach his sentencing challenge at this time. Upon remand, the district court may consider in the first instance whether its original calculation of the number of photos attributable to Cameron is still valid in light of the reversal of the convictions on Counts One, Three, Four, Five, Eleven, and Fourteen.

III. Conclusion

Before concluding, we pause to reiterate, for clarity's sake, what we have (and perhaps more importantly, what we have not) held today. Our holding today does not mean that non-testimonial business records somehow become testimonial simply because the government seeks to use them as evidence against a criminal defendant. However, if business records are testimonial, then a defendant must be given an opportunity to confront the authors of those records. What the government did in this case was seek to

[16] During oral argument, counsel for the government seemed to admit that the admission of the Yahoo! CP Reports was harmful to several counts of the indictment, but stated that the admission of the CyberTipline Reports was not. We take the government at its word that the CP Reports were harmful, but disagree with its characterization of the CyberTipline Reports, as it is evident that these were central in proving that Cameron had uploaded child pornography images on the specific dates set out in the indictment.

introduce, absent confrontation of the authors, out-of-court statements that: (1) did not exist before criminal activity was discovered; (2) stated conclusions (though perhaps obvious ones) about the meaning of underlying data; (3) were created for the express purpose of reporting criminal activity and identifying the perpetrator of that activity; and (4) were reported to a government-funded entity that serves as a conduit for passing information to law enforcement. This, we hold, the government cannot do.[17]

We **reverse** Cameron's convictions on Counts One, Three, Four, Five, Eleven, and Fourteen, and **vacate** his sentence as to those counts. We **affirm** Cameron's convictions on the remaining Counts. We **remand** to the trial court for further proceedings consistent with this opinion, including a new trial on Counts One, Three, Four, Five, Eleven, and Fourteen, if the government wishes to so proceed.

AFFIRMED in part, REVERSED in part, and REMANDED.

"Dissenting opinion follows"

---

[17] As the Supreme Court discussed recently in Williams, there are special rules that apply to testimony by expert witnesses about the conclusions they draw from underlying data. See 132 S. Ct. at 2233-35, 2239-41. Because there was no expert testimony at issue in this case related to image upload times or IP addresses (the only expert testimony, from Dr. Ricci, concerned the age of persons depicted in the images), our analysis is not disturbed by the Supreme Court's conclusions in Williams about expert testimony.

HOWARD, Circuit Judge (dissenting in part). I dissent only with respect to the majority's conclusion that the district court's decision to admit the Yahoo! reports and the NCMEC CyberTipline reports ran afoul of the defendant's Sixth Amendment Confrontation Clause protection. From my vantage, the majority is taking an unjustified step beyond what current Supreme Court precedent dictates in the developing arena of what documents bearing the hallmarks of business records and offered as evidence in a criminal trial constitute or contain testimonial statements for purposes of the Confrontation Clause. Because I do not see the documents targeted by the majority as containing a testimonial statement in the manner advanced by the appellant, I would not disturb the district court's decision to admit the documents.

The Sixth Amendment's Confrontation Clause confers upon an accused in a criminal prosecution the right to be confronted with the witnesses against him. U.S. Const. amend. VI; see Bullcoming v. New Mexico, 564 U.S. __, 131 S. Ct. 2705, 2713 (2011); United States v. Phoeun Lang, 672 F.3d 17, 21 (1st Cir. 2012). This constitutional mandate affords a criminal defendant procedural protection by guaranteeing that the reliability of certain evidence, tagged "testimonial hearsay," can be tested by cross-examining the one "bear[ing] testimony" against him. Crawford v. Washington, 541 U.S. 36, 51, 53 (2004); accord Davis v. Washington, 547 U.S. 813, 823-24 (2006). Of course, the

reliability of all evidence offered against a criminal defendant is always at the forefront of a trial court's gatekeeping role, but the Sixth Amendment guarantees the opportunity for a particular manner of testing reliability, cross-examination, for a particular type of evidence, testimonial out-of-court statements offered for the truth of the matter asserted by the declarant. See Williams v. Illinois, 567 U.S. __, 132 S. Ct. 2221, 2232-35 (2012) (plurality); Crawford, 541 U.S. at 59-60 n.9 (citing Tennessee v. Street, 471 U.S. 409, 414 (1985)). Evidence offered by the government that is an out-of-court testimonial witness statement cannot be admitted at a criminal trial unless the declarant of that testimonial statement is unavailable and the accused has had an opportunity to cross-examine the declarant on a prior occasion. See Crawford, 541 U.S. at 59 & 60 n.9; see Lang, 672 F.3d at 22.

The Supreme Court has recited various formulations of the "core class of 'testimonial' statements" as including

> (1) "ex parte in-court testimony or its functional equivalent—that is, material such as affidavits, custodial examinations, prior testimony that the defendant was unable to cross-examine, or similar pretrial statements that declarants would reasonably expect to be used prosecutorially," (2) "extrajudicial statements contained in formalized testimonial materials, such as affidavits, depositions, prior testimony, or confessions," and (3) "statements that were made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial."

Lang, 672 F.3d at 22 (quoting Crawford, 541 U.S. at 51-52) (ellipsis omitted). While the Court initially did not endorse any particular formulation as circumscribing the bounds of testimonial hearsay, see Davis, 547 U.S. at 822, it seems to have since ratified the above list, at least as being illustrative. See Melendez-Diaz v. Massachusetts, 557 U.S. 305, 309-10 (2009); Lang, 672 F.3d at 22. And in recent years, the Court has considered the scope of "testimonial" statements, particularly in the police interrogation setting, see Davis, 547 U.S. 813, and with respect to scientific reports, see Bullcoming, 131 S. Ct. 2705; Melendez-Diaz, 557 U.S. 305; see also Williams, 132 S. Ct. 2221.

In this case, Cameron argued vigorously to the trial court that the various digital images and related materials that had been derived from Yahoo!, NCMEC and Google sources must be excluded from evidence unless the government produced at trial the percipient witness who found and seized the electronic contraband and transmitted it to the government. In one pleading defense counsel posited, "[t]he figurative elephant in the room revolves around whether Mr. Cameron must be given an opportunity to confront each and every witness who supplies evidence that the government will use to prove that Mr. Cameron committed the alleged offenses." In his motion for a new trial, the defendant insisted that the "testimonial qualities" of the various evidence -- particularly the Yahoo! evidence introduced by witness Lee -- was "obvious."

Failing to persuade the trial court, the defendant now brings his constitutional plaint before us. As the majority notes, Cameron does not parse out the testimonial nature of each of the various pieces of digital and documentary evidence originating from Yahoo!, NCMEC, and Google. Instead, he takes the global position that "any report which discloses the location where evidence was seized must be testimonial." With a sweeping stroke, Cameron argues that because such reports attest to the location where the digital images themselves were found, they are "clearly testimonial statements" that are identical to a statement that "I found the drugs in the defendant's car" or "I found the gun in the defendant's garage." To test the veracity of these purported statements about location that are embedded within the reports, the appellant claims that he was entitled to cross-examine the person(s) who found the records about how, when and where the CP images were located.

I agree with the majority that the admission of evidence pertaining to the Yahoo! Account Management Tool, the Yahoo! Login Tracker data, and the Google Hello Connection logs does not implicate the Confrontation Clause. I do not, however, view the Yahoo! reports (presented in the form of receipts to the judge sitting as fact finder), and by extension the NCMEC CyberTipline

reports, as amounting to testimonial statements in the manner argued by the defendant and decided by the majority.[18]

To begin, I emphasize that the Sixth Amendment is concerned with testimonial statements that are being offered for the truth of the matter asserted. See Williams, 132 S. Ct. at 2232-35; Crawford, 541 U.S. at 59-60 n.9. And so, it is important to look to the government's purpose in admitting the Yahoo! reports.

While the defendant likens the Yahoo! reports to witness testimony of the location of contraband, the government did not offer any Yahoo! report for the truth of any averment in it that the stored images found in the particular Yahoo! photo album actually were contraband or even "suspected" contraband. Indeed, the government was clear that even the illicit descriptive "original names" of some of the image files (not assigned by a Yahoo! employee) listed in the report's table should not be relied on to assess the illegal nature of the actual digital images. Rather, the government provided the testimony of an expert in child abuse who analyzed each image in relation to the "Tanner stages" to establish that the sexually graphic images in fact depicted children within a certain age span.

---

[18] For the same reasons as the majority does, I refer solely to the Yahoo! reports when conducting the constitutional analysis here. I also note that numerous receipts of the Yahoo! reports were admitted into evidence and at times, I reference a report in the singular simply for ease in exposition.

Moreover, the appellant provides no record support to show that the district court, as the trier of fact in this case, somehow relied on the Yahoo! reports to determine whether or not the images themselves constituted child pornography. The trial court was quite clear that the documentary evidence was admitted for the purpose of providing a link between the images alleged to be child pornography that were found on the Yahoo! server, and the particular identified user name (also sometimes referred to in the evidence as "screen name" or "login name") and IP address that Yahoo! associated with that user name. The trial court also referred to the various "ISP documents" admitted into evidence in relation to the image archives as "chain of custody evidence."

Accordingly, the constitutional analysis is properly confined to whether an admitted Yahoo! report contains testimonial statements that the images listed in the report and provided as digital evidence were located in the photo album account associated with a particular user name (such as "harddude0000") and a particular IP address Yahoo! associated with that user name (such as "76.179.26.185"). Certainly, the reports reflect this location connection. But a review of both Lee's testimony explaining the process of data storage and retrieval followed by Yahoo!, as well as the reports themselves, leads to the conclusion that the Yahoo! reports do not contain any testimonial statements.

For his part, the defendant generally speaks of all of the records that accompany the digital images as "affidavits that attest to the location" of where the images were found, but he does not analyze each document type. Instead, he likens the sum of the reports in this case -- including the Yahoo! reports -- to the evidence at issue in Melendez-Diaz and Bullcoming, arguing that the records "were admitted as computer forensic evidence obtained by unknown persons using unknown methods and presented by substitute witnesses" in violation of his Sixth Amendment right to confrontation. The comparison, however, is inapt.

The heart of the testimonial hearsay in Melendez-Diaz was a certification statement akin to an affidavit made by a state forensic laboratory analyst attesting to the fact that the forensically analyzed substance was cocaine; the substance had been seized by law enforcement and delivered to the state laboratory for analysis of its contents. 557 U.S. at 308. The certificates were offered as substantive evidence to prove the truth of the assertion that the nature of the substance was actually cocaine, an assertion generated by a scientific forensic analysis specifically engaged in to produce evidence for use at a criminal proceeding. Id. at 310-11.

The circumstances of Bullcoming are similar. The testimonial statement in that case consisted of a certification by an analyst akin to a "formalized signed document" attesting to the

fact that a blood sample contained an alcohol content of "0.21 grams per hundred milliliters"; the blood had been drawn from the defendant at a local hospital in connection with a driving under the influence charge and delivered to the state laboratory by law enforcement for forensic analysis of its contents. 131 S. Ct. at 2710, 2716-17. The certificate was offered as substantive evidence to prove the truth of the assertion as to the level of alcohol content in the blood sample, an assertion generated by a scientific forensic analysis specifically engaged in to produce substantive evidence for use at a criminal trial. Id. at 2711, 2713, 2716-17.

Here, the defendant is left to argue that the purported statement in a Yahoo! report offered for its truth is that the digital images were found in the Yahoo! photo album tied to the identified user name and the associated IP address. For its part, the majority seizes on the IP addresses identified in the Yahoo! reports because in one instance a different IP address was recorded in the Account Management Tool for the identified user name. The majority surmises that both the government and the district court took the IP address identified in a Yahoo! report to be the one from which the most recent image of child pornography had been uploaded into a Yahoo! photo album. From this the majority concludes that the government used the Yahoo! reports to tie the defendant to the specific IP addresses from which child pornography images were uploaded. Even so, I part ways with the majority

because the link in any given Yahoo! report between the incriminating images and the accompanying user name and IP address is not a testimonial statement.[19]

To the extent the connection between the identified user name, the associated IP address, and the digital images archived from that user's photo album can be deemed a declarant statement, that location connection existed well before Yahoo! even received the customer complaint about the content of the images associated with the screen name "lilhottyohh". Indeed, the thrust of Lee's testimony was that the storage of the digital images and the associated account data on the Yahoo! servers was an essential part of the Yahoo! photo album service. The record indicates that the computer systems and retrieval tools for locating images in any given user's photo album (along with stored account information gathered with the archive such as the associated IP address) were the same as those Yahoo! uses to locate all information stored about a user on the servers for its ordinary business functions. It is helpful to amplify the record on this point.

As the majority notes, Yahoo! is an Internet Service Provider portal which, as Lee explained, is in the business of

---

[19] The majority begins its discussion on the testimonial nature of the reports by examining their facial features, focusing on the term "suspect" that is contained in some "fields" that list certain types of information, such as "Suspect IP Address." I think it more likely that "suspect" is used as an adjective in the reports to delineate the suspicious address and user names, not, as the majority says, as a noun targeting a specific person.

providing several internet services to its users, such as internet searching, email, "messenger," and (as of the time of the criminal conduct at issue) a photo album service. Various types of information or data relating to Yahoo! users and the services that each user employed are stored on servers. Such stored information includes emails, email "address books," "friends" lists, user registration information, and login history. Data pertaining to the photo album service -- the stored digital images -- was handled no differently. This service allowed a Yahoo! user to load digital images from various sources -- such as an email attachment or an internet site -- to an internet photo album associated with that user's Yahoo! account. The service enabled a user to store digital images on a Yahoo! server and then easily share the stored photo album with other internet users by sending them the URL link to the album's internet location. Once loaded to the photo album, the digital images remained automatically stored on Yahoo! servers unless and until the user deleted them (although Yahoo! also could eliminate access to the images by deactivating a user's account).

Lee's testimony shows that each type of stored information or data pertaining to each Yahoo! user or "screen name" is accessed by Yahoo! employees using the same methodology. The method consists of a Yahoo! employee, such as one in the customer care department, inputting a user name into a particular retrieval tool associated with certain types of stored information, such as

the Account Management Tool or Login Tracker. The computer tool then automatically accesses the stored information related to that tool and displays it for the Yahoo! employee to review. Some tools compile various data; the Account Management tool, for example, collects the IP address recorded when a user first creates an account and the registration information provided by that user, among other stored information. Lee testified that these systems of data storage and retrieval are relied upon by Yahoo! to provide reliable and accurate data on customer accounts in order to conduct its business as an ISP. Lee explained that the same systems and tools also are used to access stored data pertaining to users when Yahoo! responds to a search warrant or any other legal process.

There is absolutely no indication in this record that the archives for the digital images from photo albums associated with the various Yahoo! user names in this case (as well as the IP addresses and other account data included with each image archive) were created, generated, or developed outside of this routine administrative methodology for retrieving stored user account data -- a process which itself necessarily links the location of the retrieved stored data to the user name inputted. That the retrieved digital images stored on the server were captured electronically for purposes of transmitting them to the legal department is no different from the location connection created between data and user each time other types of stored data are

retrieved and printed (or otherwise transmitted) for review, such as a user's login history, "friends" list, or email "address book." In short, the purported location statement made by the stored image archive itself (along with other accompanying stored user data), and reflected in the Yahoo! reports, was not made for the primary purpose of establishing or proving a fact or past event for criminal prosecution, but for the very functioning of the ISP business operations. See generally Williams, 132 S. Ct. at 2243 ("the primary purpose of the [scientific] report, viewed objectively, was not to accuse petitioner or to create evidence for use at trial"); Bullcoming, 131 S. Ct. at 2714 n.6 ("To rank as 'testimonial,' a statement must have a primary purpose of establishing or proving past events potentially relevant to later criminal prosecution." (internal quotation marks and brackets omitted)); Melendez-Diaz, 557 U.S. at 324 (noting that business record "having been created for the administration of an entity's affairs and not for the purpose of establishing or proving some fact at trial . . . are not testimonial").[20]

Also, Lee testified that the Yahoo! reports electronically transmitted to NCMEC comprise the same image archives captured by a customer care employee (along with stored account information gathered with the archive); the only difference

[20] The "primary purpose" inquiry of the statement's "testimonial" nature focuses on the declarant's purpose in making the statement. See Davis v. Washington, 547 U.S. 813, 822-23 n.1, 826-28 (2006).

is that any images that the Yahoo! legal department employee does not suspect as containing child pornography are not included in the report. Thus, the location link between the images and the user's account is simply memorialized by an administrative process when the archive is created, which is simply repeated in the Yahoo! report sent to NCMEC. Then, a Yahoo! report receipt is automatically generated via computer, including the sequential list of numeric "Legal Archive Tool" image names.

I disagree with the majority's conclusion that the Yahoo! reports are distinct from the other documents targeted by the defendant in this case, such as the Account Management Tool, because "they convey an analysis that was performed using pre-existing data" and make "an entirely new statement reflecting [] conclusions" drawn from such an "analysis." I suppose that this could be the case if the government were using the Yahoo! reports for the truth of an assertion that the images in fact were child pornography or suspected child pornography. But, as I began, the government did nothing of the sort. The conveyance of any analysis that a Yahoo! employee performed to deem some images in certain user photo albums to be suspect was not the purpose of the exhibits' admission. And, I might add, it is the purported location statement -- linking the images (and other stored data) to the identified user name and the associated IP address -- to which this appellant objects. The record reflects that the location

connection was not generated by a forensic analysis performed to produce substantive evidence at a criminal trial in the manner that was central to the testimonial nature of the certification reports in both Melendez-Diaz and Bullcoming.

The majority emphasizes that (1) the retrieval process for the digital images in this case began once Yahoo! received a tip associating images of child pornography with a particular user's account, (2) the particular Yahoo! reports at issue were generated as part of a process that Yahoo! developed to comply with its legal duty to report any apparent violation of federal child pornography laws to NCMEC, (3) the reports were delivered to NCMEC, which operates, in part, as a type of clearinghouse for ISP reports to law enforcement regarding suspected child pornography, and (4) the actual Yahoo! report documents (the receipts) did not exist before the discovery of the suspected criminal activity. These circumstances do not alter the conclusion that the putative statement that there is a location connection between user and stored data (including digital images and information relating to the Account Management Tool or the Login Tracker) pre-existed any customer complaint or other event that would trigger the retrieval of such data, and the process for retrieving the various stored data is not performed through a forensic analysis engaged in to produce substantive evidence at a criminal trial. And, as I have explained, any new statement about the content of the images

containing suspected child pornography was not offered for the truth of the matter asserted.

In summary, while I agree with the majority that evidence does not escape testimonial hearsay status under the Confrontation Clause simply because it may otherwise bear the characteristics of a business record, I do not believe that the location link displayed in the Yahoo! reports amounts to a testimonial statement under current Supreme Court precedent or under our own cases. I disagree with the appellant that the holdings in Melendez-Diaz and Bullcoming compel a conclusion that admission of the various "accompanying reports" -- which he labels as "computer forensic evidence" -- required an opportunity to cross-examine the person(s) who actually located the stored digital images and created a corresponding archive associated with each user name photo album.[21] And, I see nothing in the most recent Supreme Court discourse on the Confrontation Clause to alter my view on the import of Melendez-Diaz and Bullcoming holdings under the facts of this record. See generally Williams, 132 S. Ct. 2221..

---

[21] The defendant also suggests in his brief that his Sixth Amendment concerns would have been allayed had the government presented live testimony of a Yahoo! computer technician to explain and verify the accuracy of the company's software tools used to retrieve the digital images and account data. This tack, however, essentially concedes that the reports contain no witness testimony whatsoever and reduces his argument to one of authentication. If this is the appellant's strategy, then the majority's footnote remark about Rule 803(6) probably suffices for the Yahoo! reports as well. In the end, though, I make no judgment on authentication because the issue before us is confined to the Sixth Amendment.

I respectfully dissent from the majority's conclusion that admission of the Yahoo! reports and NCMEC CyberTipline reports[22] violated Cameron's rights under the Confrontation Clause, and so I would affirm the appellant's conviction on all counts.

[22] With respect to the NCMEC CyberTipline reports, the majority concludes that the government appeared to rely on these documents as the sole evidence establishing the upload dates and times of the illegal images (the so-called "Image Upload Data"). The majority also appears to assess the record evidence to determine whether the government appropriately established through this NCMEC evidence the transporting-by-uploading element charged in the indictment. There is no need to consider these issues because the timing of image uploading is not part of the appellant's Sixth Amendment argument. There is also no need for me to separately analyze whether the NCMEC CyberTipline reports contain a testimonial statement that was offered for the truth of the matter asserted. For present purposes I take the government at its word that such evidence essentially parroted the substance of the Yahoo! reports. Again, I note that the defendant makes no attempt to parse the two types of documents when advancing his Sixth Amendment plaint.