

FILED
Clerk
District Court

IN THE UNITED STATES DISTRICT COURT NOV 20 2012
FOR THE NORTHERN MARIANA ISLANDS

for the Northern Mariana Islands
By _____

UNITED STATES OF AMERICA,

Case No.: 1:12-CR-00017 (Deputy Clerk)

Plaintiff,

vs.

THOMAS WEINDL,

Defendant.

**MEMORANDUM OPINION AND ORDER
DENYING IN PART AND GRANTING IN
PART DEFENDANT'S MOTION TO
SUPPRESS AND DENYING
DEFENDANT'S MOTION TO DISMISS**

I. INTRODUCTION

Before the Court is Defendant Thomas Weindl's motion to suppress evidence and, in the event the suppression motion is granted, to dismiss the indictment with prejudice.¹

Weindl is charged with two counts of receiving child pornography and two counts of accessing child pornography with intent to view it. The charged conduct is alleged to have occurred on or about June 15 and June 18, 2012. Weindl seeks to suppress (1) information regarding possible child pornography Internet searches and downloads obtained from a laptop computer without a warrant, and (2) statements he made to law enforcement agents on June 28, 2012.

The suppression motion turns on the intersection of the personal and professional lives of two individuals: Thomas Weindl, the former principal of Whispering Palms School in Saipan, Commonwealth of the Northern Mariana Islands ("CNMI"); and Joseph Auther, a special agent of the Federal Bureau of Investigation ("FBI") who had children enrolled in

¹ Initially, on October 4, 2012, Defendant moved only to suppress evidence (*see* ECF No. 29). Later the same day, he filed an Errata in which he additionally moved to dismiss the indictment (*see* ECF No. 30).

1 Whispering Palms. Auther monitored his eldest son's computer activity by installing spyware
2 on a laptop purchased by the Public School System ("PSS") and issued to the boy for school-
3 related use. The spyware sent Auther e-mails listing his son's website visits and keystrokes.
4 When his family was preparing to leave Saipan, Auther returned the laptop to Weindl at the
5 school but did not remove the spyware. A few days later, he received e-mails indicating that
6 someone was using the laptop to visit websites involving child pornography. The ensuing
7 investigation led to Weindl's questioning and arrest.
8

9 In response to the motion, the Government filed an opposition brief (ECF No. 34), to
10 which Weindl replied (ECF No. 39). In his reply, Weindl raised a new argument, that Auther's
11 conduct violated federal wiretap laws and should be suppressed on statutory grounds. The
12 Government did not object to the Court's considering this argument, on the condition that it
13 have adequate time to respond in writing. Subsequently, the Government filed a memorandum
14 on the wiretap issue (ECF No. 44), to which Weindl responded (ECF No. 46).
15

16 The matter came on for an evidentiary hearing on October 25, 2012. Over four days, the
17 Court heard testimony on behalf of the Government from Auther as well as FBI Special Agent
18 Edmund Ewing and Tim Thornburgh, the federal programs officer at PSS. The defense
19 presented testimony from Clarence "Bud" White, the owner of a computer service business in
20 Saipan. Weindl himself submitted two sworn declarations (ECF Nos. 29-2 and 38) but did not
21 testify.
22

23 Having reviewed all the testimony, declarations, and exhibits, and having heard
24 argument of counsel for both parties, the Court now DENIES the motion to suppress with
25 respect to the eBlaster e-mails and reports as well as the statements Weindl made during the
26 June 28 interview in his office at the school. The Court GRANTS the motion to suppress with
27
28

1 respect to statements made in response to police questioning after Weindl was formally taken
2 into custody outside his office and without adequate advisement of his constitutional rights.
3 Because substantial evidence remains available to the Government in its case in chief, the
4 motion to dismiss is DENIED. The reasons for these determinations are explained herein.

5 **II. BACKGROUND**

6
7 The Court finds the following facts based on the testimony, declarations, and exhibits
8 introduced into evidence at the motion hearing.

9 **A. Search of the Laptop Computer**

10 Joseph Auther is an FBI special agent. He is married and has three school-age sons. His
11 eldest son, a seventh grader at Whispering Palms School in Saipan, had been issued a laptop
12 computer obtained by PSS through a federal grant. In July 2011, Auther installed on the laptop
13 a commercial software product, eBlaster, for the purpose of monitoring his son's Internet use.
14 The company that produces eBlaster is SpectorSoft. Auther had heard about eBlaster from a
15 friend, a retired FBI agent who had installed it on his own child's computer. Auther had never
16 used eBlaster in FBI investigations.
17

18
19 On his home computer, Auther visited the SpectorSoft website and purchased eBlaster
20 with his personal credit card. After he had installed the program on the laptop, eBlaster sent
21 messages to Auther's personal e-mail account several times a day. The e-mails contained
22 reports listing any websites and chat rooms that had been visited and the keystrokes that had
23 been entered on the laptop. Auther accessed his e-mail through Microsoft Outlook. The inbox
24 listing would show that a message had been received from eBlaster and would give the subject
25 as "Report," followed by the date and time span of covered activity. (See Ex. 2.)
26
27
28

1 A sister court has provided a succinct explanation of how eBlaster works. It accords
2 with descriptions of the software given in testimony at the hearing on this motion, so the Court
3 adopts it:

4 eBlaster is a computer software program that can perform various
5 spyware functions. It can record every keystroke made on the computer on which
6 it is installed. It can also keep track of all websites visited and all applications
7 used on that computer, and it can capture screenshots of instant messages and
8 cached webpages. In addition, it can be directed to compile a report of this
9 information at selected time intervals and send that report to a designated third
10 party email address. Further, it can be directed to automatically forward copies of
11 incoming email accessed on that computer to the third party email address. Each
12 individual email is sent separately and independently from the eBlaster reports.
13 eBlaster can also forward to this third-party email address copies of instant
14 messages or “chat” messages as they are occurring.

15 *Klumb v. Goan*, 2012 U.S. Dist. LEXIS 100836, *6 (E.D. Tenn. July 19, 2012).

16 Author did not tell his son that he had installed eBlaster. No icon or other sign appeared
17 on the laptop’s user interface to indicate that eBlaster was installed.²

18 In October 2011, Author was having technical difficulties with eBlaster and called
19 SpectorSoft’s customer support line. In the course of fixing the problems, the technician
20 walked Author through the steps to uninstall and reinstall the program. (*See* Ex. C, record of
21 SpectorSoft service call.)

22 In April 2012, Author learned he was being relocated to the FBI’s Denver office. By
23 June 15, in preparation for the move, all Author’s CNMI cases had been transferred to other
24 agents, and Author was not conducting any ongoing investigations or looking to open new ones.

25 ² “Even with an anti-virus program, eBlaster generally cannot be detected on the computer on which it is
26 installed unless a person knows the ‘hot key’ combination, the three key combination which must be
27 depressed simultaneously in order to make eBlaster’s dialog box appear on the computer screen. Once
28 the dialog box appears on the screen, a username and password is required in order to go to the eBlaster
control panel. At the control panel, the user chooses the settings for eBlaster to provide the desired
information.” *Klumb* at *6. Author testified that he knew to press a key combination in order to install
an update or to change settings for the frequency of activity reports.

1 On or about June 6, Auther notified Thomas Weindl, the principal and corporate director
2 of Whispering Palms, that he would have the laptop serviced and have all his son's files,
3 programs, and games wiped from the hard drive before returning it to the school. He did not tell
4 Weindl that he had installed eBlaster.

5 Auther had known Weindl for about five years. They saw each other almost daily
6 during the school year and went on the annual school camping trip together. Auther frequently
7 stopped by Weindl's office. Although he and Weindl did not socialize, Auther considered
8 Weindl a friend. When Weindl got married in January 2012, Auther's wife gave a reading at
9 the ceremony.
10

11 The first step Auther took to service the laptop was to bring it into the FBI office and ask
12 fellow agents for advice on how to wipe it clean. They tried to remove all the files but were
13 unsuccessful. Next, on June 8, Auther asked a local computer store to repair a scratched screen
14 and wipe off all the files on the laptop's hard drive. The store's service order (Ex. 1) lists the
15 work to be done as "Reimage" and the work performed as "Clean out files." Auther did not tell
16 the technician about eBlaster, but he expected that the cleaning would eliminate the program.
17 That evening, he gave the laptop to Weindl at Whispering Palms and told him something to the
18 effect that it had been wiped clean and the files had been deleted. He did not mention the
19 eBlaster spyware to Weindl.
20
21

22 For the next week, Auther received no e-mails generated by eBlaster. Then, in the late
23 afternoon of Friday, June 15, Auther noticed that he had received a series of eBlaster e-mails.³
24 He clicked on the subject lines and read the reports. The reports alluded to Internet searches for
25
26

27
28 ³ Four e-mails with "sent" dates on or before June 15 were introduced into evidence: (1) sent June 14, 2012, at 12:29 p.m.; (2) sent June 15, 2012, at 8:00 a.m.; (3) sent June 15, 2012, at 11:00 a.m.; and (4) sent June 15, 2012, at 2:58 p.m. (See Ex. 2.)

1 child pornography. Auther's initial reaction was shock that his son was visiting sexually
2 explicit websites. Only on reflection did he realize that he had already returned the laptop to the
3 school. He wondered if the sudden activity was the result of a computer virus that had infected
4 his home desktop, which he had used to purchase eBlaster, or if another student had accessed
5 the laptop at Whispering Palms. He did not ask his son if he had taken the laptop back from the
6 school and was using it again.

8 Auther also wondered if Weindl himself was using the laptop to access child
9 pornography. Some of the websites appeared to involve young Asian girls having sex with
10 older men. Auther was aware that in January, Weindl had married a Korean woman, and he
11 now had an 11-year-old Korean stepdaughter.

13 Early in the evening of June 15, Auther called his wife to get Weindl's cell phone
14 number, and then called Weindl. Auther pretended to be interested in purchasing the laptop and
15 asked Weindl who he had given it to. Weindl told Auther he had returned the laptop to PSS.
16 Auther did not tell Weindl that eBlaster was installed or that he had received reports of child
17 pornography searches on the laptop. Auther testified that he did not want to raise concerns in
18 Weindl's mind about who was using the computer or about a possible investigation involving
19 Whispering Palms teachers and students. Weindl told Auther he would not be able to buy the
20 laptop from PSS because it was federally funded. Auther found Weindl's explanation credible.
21 He did not mention the incident to his colleagues at the FBI or to other law enforcement
22 officials. However, he was concerned that the Internet activity might mean that a child molester
23 was operating at Whispering Palms. He was aware that a former coach at Pennsylvania State
24 University had just been convicted on child molestation charges, and he was determined not to
25 allow similar conduct to go undetected at Whispering Palms.

1 The following Monday, June 18, Auther went to the PSS office around ten in the
2 morning and spoke with Joseph Torres, PSS's technology coordinator. Auther identified
3 himself to Torres as an FBI agent. Auther testified that he showed his FBI credentials because
4 he figured Torres would not speak about the laptop matter with just any parent. Ewing testified
5 that an FBI agent is only supposed to use FBI credentials in relation to the agent's job.
6

7 Auther told Torres that he was looking into a student laptop that had purportedly been
8 turned into PSS, and that he was concerned with inappropriate activity on the laptop. Torres
9 informed Auther that the schools never returned the laptops to PSS but simply redistributed
10 them within each school to new students. The only school to have returned laptops was Calvary
11 Christian Academy, which had recently closed down.
12

13 Tim Thornburgh is the federal programs director at PSS responsible for the laptop
14 program. He testified that the laptops are purchased for students in grades 7–12 with money
15 from federal grants. The laptops are provided to both public and private school students. PSS
16 developed a manual (*see* Ex. 6) to educate parents and students on the use of the laptops for
17 homework and self-directed learning. Parents and students sign a contract when they receive
18 the laptops. The laptops are the property of PSS. If the student takes good care of the laptop, it
19 is gifted to the student upon graduation. During the student's school career, the laptop remains
20 the property of PSS. Thornburgh met monthly with public and private school principals to
21 discuss the laptop program and the agreement.
22

23 After leaving PSS, Auther visited his Internet service provider in hopes of obtaining
24 information about an Internet Protocol ("IP") address that appeared in the eBlaster reports. The
25 support staff refused to disclose the information. Auther was able to determine from them,
26 however, that the eBlaster activity was not coming from his home. Auther testified that he may
27
28

1 have shown his FBI credentials to the support staff. He conceded that to ask for information
2 about someone else's IP address would have crossed the line into an official investigation.

3 Around noon, Auther spoke with his wife. In his testimony, he was unsure whether he
4 talked to her on the phone or stopped by their house. He learned that they had received a new
5 eBlaster report on Internet activity involving child pornography.⁴ It is not clear from the record
6 whether he or his wife opened the report or how much information they gleaned from it.
7

8 That afternoon, shortly after two o'clock, before going to the FBI office, Auther drove
9 by Whispering Palms. He noticed that Weindl's car was parked at the school. He did not stop
10 in, but called Weindl on the cell phone. Auther reiterated his desire to find the laptop and
11 mentioned his concern that there may be some inappropriate content on it. Weindl responded
12 that he had done some checking of his own; that some "hanky panky" was going on at PSS; that
13 he had determined that the laptop had been recirculated; and that he had spoken to some PSS
14 officials and was looking into the matter on his own. Auther did not confront Weindl with the
15 fact he had visited the PSS offices and knew that Weindl had lied about returning the laptop
16 there.
17
18

19 The telephone conversation strengthened Auther's suspicions of Weindl. When he got
20 to the FBI office, he reported about the illicit Internet activity and Weindl's possible
21 involvement to Special Agent Ewing. He also notified the CNMI Attorney General about his
22 concerns and asked that someone from child protective services check on Weindl's
23 stepdaughter.
24
25

26
27 ⁴ Two e-mails sent June 18, 2012, were introduced into evidence: (1) sent at 11:57 a.m., and (2) sent at 2:57 p.m.
28 The first of these e-mails reports activity from "Fri 03:10pm to Mon 12:09pm." (See Ex. 2a.) The second one
reports activity from "Mon 12:09pm to 03:09pm." (See Ex. 2.) Both reports involved child pornography. It is not
clear how a report purportedly sent at 2:57 p.m. could report activity that supposedly occurred 12 minutes later.
The discrepancy is not relevant, however, to the disposition of this motion.

1 After June 18, Auther stopped receiving e-mail reports of Internet activity from eBlaster.
2 On June 22, he forwarded the eBlaster e-mails to Special Agent Ewing. Ewing interviewed
3 Auther and took steps to open a formal investigation, including contacting his supervisor and a
4 federal prosecutor.

5 **B. FBI Questioning of Weindl**
6

7 On the morning of June 28, 2012, Auther and Ewing came to Weindl's office at
8 Whispering Palms. They drove there in an unmarked FBI vehicle and were in civilian clothes
9 devoid of any FBI insignia. They carried concealed handguns. They had obtained a search
10 warrant for Weindl's office and the school but hoped to talk with Weindl before serving it.
11 They had not made an appointment with Weindl or been invited to visit him.
12

13 When the agents arrived at the school about 10:45 a.m., Auther opened the door of
14 Weindl's office and saw that Weindl was in a meeting with a school parent. Ewing and Auther
15 waited outside at picnic tables for about five minutes while Weindl and the parent talked in
16 Weindl's office. Ewing testified that at this point, Weindl was the sole suspect of the
17 investigation, but that the FBI did not have probable cause to arrest him prior to interviewing
18 him.
19

20 When Weindl and the parent came out of the office, the four men engaged in small talk
21 for a few minutes. (Ewing happened to know the parent from activities unconnected with the
22 school.) After the parent left, the agents told Weindl they wished to speak about the missing
23 laptop. When a maintenance crew started making noise with power tools, they moved into
24 Weindl's office. From the record, it is not clear whether Weindl invited them in or one of the
25 agents suggested they go in. Ewing and Auther closed the door behind them. Weindl had no
26 access to the door without walking past the agents.
27
28

1 Weindl's office was a small room, about six feet wide and twelve feet long. It had one
2 window, which overlooked a picnic area. The room had only two chairs: one behind the desk
3 and one for visitors. When the three men came in, Auther offered to stand, but Weindl went
4 into a classroom and brought a third chair for him. Weindl sat at his desk. Ewing sat at a small
5 table facing Weindl. Auther sat behind Ewing, directly in front of the closed door, as the room
6 was too narrow for the two agents to sit side by side. Auther described the room as "cramped."
7 Weindl said he felt "cornered." (First Decl., ECF 29-2, ¶ 15.)

9 Weindl's office had two doors. The outer door was the entryway from the picnic area,
10 and the inner door led to a classroom. Auther was between Weindl and both doors. The outer
11 door remained closed throughout the interview.

13 Ewing led the interview. He told Weindl that they were investigating the disappearance
14 of the PSS laptop because it had been obtained with federal funding. He said that if Weindl did
15 not cooperate and provide specific and accurate information, a larger investigation would have
16 to be undertaken, which would involve questioning school staff and parents. In response,
17 Weindl apologized for not having told the truth from the beginning, when Auther first called
18 him on June 15. He said he was embarrassed that the laptop had gone missing from his office
19 and so had lied about the disappearance. Ewing asked Weindl when the laptop had disappeared,
20 and Weindl was unable to give a specific date. Ewing then told Weindl that inappropriate
21 Internet activity had been observed on the laptop, and that it was important to understand who
22 had been using it. He repeated that they would have to start interviewing members of the
23 community if Weindl was not more forthcoming. Weindl then admitted that he had viewed
24 pornography on the laptop for about three days before destroying the unit and throwing the
25 pieces in the jungle.
26
27
28

1 The entire interview lasted between 45 minutes and one hour. It was not recorded. The
2 agents testified that throughout the interview Ewing's demeanor was calm and his tone was
3 conversational, and Ewing never raised his voice. Ewing testified that he made no threats or
4 promises. However, he acknowledged that he exploited Weindl's fear of a wider public
5 investigation to encourage Weindl to speak honestly, and that he assured Weindl he would share
6 information that Weindl provided only with other FBI agents and federal prosecutors.
7

8 Weindl perceived Ewing's questioning to be "quite threatening and frightening in
9 nature." (First Decl. ¶ 19.) He felt "trapped" and without a choice but to respond or be
10 immediately arrested. (*Id.* ¶ 20.) He did not feel free to refuse to answer questions or to end the
11 interview. (*Id.* ¶ 21.)
12

13 At no point before or during the interview did Ewing or Auther advise Weindl of his
14 constitutional rights or tell him that he was free to leave. Weindl never asked to take a break or
15 leave the room. He never asked the agents to stop questioning him and never requested an
16 attorney. At one point, when Weindl had become more forthcoming about his activities on the
17 laptop and seemed embarrassed, Auther asked him if he wanted him (Auther) to leave the room.
18 Auther thought that given their friendship, Weindl might be more comfortable talking to Ewing
19 alone. Weindl declined the offer.
20

21 After the interview, the three men walked out of the office. Auther and Weindl waited
22 at the picnic tables while Ewing went to his car. Ewing called a federal prosecutor on the
23 telephone and the decision was made to arrest Weindl.
24

25 Ewing gave Weindl an advice of rights form (Ex. 3), which Weindl read and signed.
26 Weindl maintains that he was told to sign the form and did not read it carefully because he was
27 upset. (First Decl. ¶ 22.) Other FBI agents were now also present. Ewing testified that because
28

1 they were in public, and out of concern for Weindl's privacy, he did not read the rights form to
2 Weindl aloud but gave it to him to read silently.

3 Before signing the form, Weindl agreed, both orally and in writing (Ex. 4), to allow the
4 agents to search his residence and any computers at the residence. After signing the form,
5 Weindl described the location where he had disposed of the laptop. He agreed to get in the
6 agent's car and go look for it. Weindl was patted down and put in the back seat of an FBI
7 vehicle, where he sat alongside another agent. Weindl was not handcuffed. Ewing drove.
8 Weindl directed Ewing to an area at the top of Navy Hill. Ewing spent about 20 minutes
9 searching but did not locate any pieces of the laptop. Weindl was then taken to the U.S.
10 Marshals Office and booked into custody.
11

12 **III. DISCUSSION**

13 **A. Suppression of eBlaster Reports**

14 The Fourth Amendment of the United States Constitution protects persons against
15 unreasonable searches and seizures of their home, property, papers, and effects. A search
16 occurs in cases involving common-law trespass or "when government officers violate a person's
17 'reasonable expectation of privacy.'" *United States v. Jones*, 132 S.Ct. 945, 949–50 (U.S. 2012)
18 (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). Thus, for a
19 person to invoke the protections of the Fourth Amendment, a search must be the product of
20 government action, and the aggrieved person must have a reasonable expectation that the
21 information seized would remain private—commonly referred to as Fourth Amendment
22 standing.
23

24 //

1 1. Whether the Seizures Were the Product of State Action

2 The Government asserts that because Auther was not acting in his capacity as an FBI
3 special agent when he installed eBlaster on his son's laptop, the seizure of evidence against
4 Weindl was not the product of a government search. (Opp'n at 7.) Searches and seizures
5 "effected by a private individual not acting as an agent of the Government or with the
6 participation or knowledge of any governmental official" are not constrained by the Fourth
7 Amendment. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (quoting *Walter v. United*
8 *States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)). In cases where the seizure was
9 made by a private person, the burden is on the defendant to establish government involvement.
10 See *United States v. Snowadzki*, 723 F.2d 1427, 1429 (9th Cir. 1984). There must be "some
11 degree of governmental knowledge and acquiescence" in a private person's actions to bring the
12 search under Fourth Amendment scrutiny. *United States v. Sherwin*, 539 F.2d 1, 6 (9th Cir.
13 1976). In close cases involving something more than a complete absence of governmental
14 participation but less than overt state action, the court must examine the facts and circumstances
15 to determine "(1) whether the government knew of and acquiesced in the intrusive conduct; and
16 (2) whether the party performing the search intended to assist law enforcement efforts or further
17 his own ends." *United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994) (quoting *United States*
18 *v. Miller*, 668 F.2d 652, 657 (9th Cir. 1982)).

19 Typically, in cases where the existence of state action is at issue, the person who
20 conducted the search was a private citizen, not employed by law enforcement, who shortly
21 before or after the search had reported a suspicion of criminal activity to police. That is so in all
22 the cases cited in the Government's Opposition: see *United States v. Cleaveland*, 38 F.3d 1092
23 (9th Cir. 1994) (utility company employee reported anonymous tip about power diversion to
24
25
26
27
28

1 police); *Miller* (private citizen relayed tip on stolen trailer to police); *Reed* (room search by
2 hotel manager); *Sherwin* (search of cartons by truck terminal manager); *United States v. Shetty*,
3 171 Fed. Appx. 561 (9th Cir. 2006) (business documents obtained by private parties and turned
4 over to law enforcement agents); *Snowadzki* (search of co-worker's papers by employee of
5 private company); *Walther*, 652 F.2d 788 (9th Cir. 1981) (search of overnight case by airline
6 employee).

7
8 When the actor is an off-duty law enforcement officer, however, the initial inquiry must
9 be whether he was acting "under color of state law." See *United States v. McGreevy*, 652 F.2d
10 849, 851 (9th Cir. 1981) (search of package by city police officer moonlighting as private
11 security consultant); *Traver v. Meshriy*, 627 F.2d 934 (9th Cir. 1980) (detention of bank
12 customer by off-duty police officer employed as teller). If a government officer "does not act
13 within his scope of employment or under color of state law, then that government officer acts as
14 a private citizen." *Van Ort v. Estate of Stanewich*, 92 F.3d 831, 835 (9th Cir. 1996).

15
16 Author's actions were under color of state law if they were "in some way related 'to the
17 performance of his official duties'" or "pursuant to [a] government or police goal." *Id.* at 838
18 (quoting *Martinez v. Colon*, 54 F.3d 980 (1st Cir. 1995)). Author's installation of eBlaster on
19 the laptop in June 2011 was unrelated to the performance of his duties as an FBI special agent.
20 His intent was solely to monitor his son's Internet activities. He had no reason to believe that
21 anyone other than his son, to whom Whispering Palms had issued the PSS laptop, would use the
22 computer during the period when it was loaned out to the boy. Author was acting as a devoted
23 father, not a law enforcement officer.

24
25 The circumstances changed, however, when Author returned the laptop to Whispering
26 Palms. If Author had intentionally left eBlaster on the laptop in order to track the activities of
27
28

1 the next user, knowing that he would be duty-bound to report any observed criminal conduct,
2 his continued receipt of eBlaster reports might be in pursuit of a police goal and therefore
3 constitute a Fourth Amendment search. But the evidence suggests that Auther left eBlaster on
4 the laptop inadvertently. When he gave the laptop to a service technician for reimaging, he did
5 not mention the eBlaster software, let alone direct the technician not to disturb eBlaster. It
6 appears that Auther did not care whether eBlaster remained on the laptop or not. The fact that
7 Auther was preparing to relocate his family to the mainland makes it all the less likely that he
8 was privately, without direction from his superiors, launching a sting to uncover misuse of
9 federally funded school computers on Saipan. In all likelihood, he had other things on his mind.

11 Weindl maintains that even if Auther did not mean to leave eBlaster on the laptop, his
12 act of opening the eBlaster e-mails converted an inadvertent search into an intentional one.
13 (Reply at 7.) He points out that the subject lines showed that the reports covered a period of
14 time (June 9–14) after Auther’s son no longer had possession of the laptop. The conclusion he
15 draws is that Auther “did not have a justifiable basis (private interest or otherwise)” for viewing
16 the contents of the report. (*Id.*)

19 This argument is not persuasive. The search was the gathering of information by
20 eBlaster, not the viewing of the contents. The analysis would be no different if Auther had
21 turned the reports over to other law enforcement officers without having read them. However
22 intentional the act of opening the e-mails may have been, the searches were still, at this
23 juncture, inadvertent. The Court therefore finds that the initial data received from eBlaster and
24 viewed by Auther on Friday, June 15, 2012, prior to Auther’s contacting Weindl, are not the
25 product of a search conducted under color of state law.

27 //
28

1 Neither would the initial eBlaster reports come under the Fourth Amendment via the
2 two-part test for private-party searches. Even if Auther “acquiesced in the intrusive conduct”
3 when he failed to direct the service technician to remove eBlaster, the intrusive conduct – the
4 installation of eBlaster – was not by the government, but by Auther the private citizen. As for
5 the second prong of the test, there is no evidence that Auther intended to further a law
6 enforcement purpose by keeping eBlaster on the laptop. Therefore, Defendant Weindl has
7 failed to carry his burden to show that he should be accorded Fourth Amendment protection
8 from the private-party eBlaster search.
9

10 The same cannot be said for the eBlaster reports that were generated after Auther called
11 Weindl on the evening of June 15. By that time, Auther knew that someone may have been
12 viewing illicit material on the laptop. He suspected Weindl even before he called him. When
13 he did call, he hid his real concern about the laptop’s usage behind a pretense that he was
14 interested in purchasing the computer. After the call, he did not uninstall or disable eBlaster,
15 even though as a private citizen he was under no obligation to continue monitoring an unknown
16 person’s offensive Internet activities. He did not immediately call his colleagues at the FBI and
17 hand the investigation over to them – conduct that might have indicated Auther wanted to
18 maintain a separation between his private self and his public persona as a law enforcement
19 officer. After Weindl told Auther that he already delivered the laptop to PSS, Auther continued
20 his investigation into the child pornography website searches. Auther testified that in his mind,
21 he was still concerned that the searches may point to his son. He was also concerned that
22 someone within PSS may be using the laptop for these illegal searches. At the PSS offices, he
23 showed his FBI badge. At the Internet service provider, he relied on the fact that he was known
24 to be an FBI agent to seek information about IP addresses. The totality of the circumstances
25
26
27
28

1 shows that at this point, Auther's actions were related to his official duties and in pursuit of a
2 police goal. Although a formal FBI investigation had not been opened yet, Auther was now
3 acting under color of law. Therefore, the searches that generated eBlaster reports after the
4 initial phone call to Weindl are subject to Fourth Amendment scrutiny.

5 The government asserts that even if Auther's conduct constituted state action, his
6 discovery of the illicit Internet activity through eBlaster e-mails was accidental and therefore
7 does not come under the Fourth Amendment. In support of this theory, the Government relies
8 on *Thompson v. United States*, 382 F.2d 390 (9th Cir. 1967). In *Thompson*, two police officers
9 and a private security guard questioned Thompson in his hotel room about suspicious cashing of
10 travelers checks. *Id.* at 391–92. During the questioning, the security guard straightened a
11 picture on the wall and a small packet fell out from behind the frame. *Id.* One of the police
12 officers opened the packet and found marijuana. *Id.* The police then arrested Thompson on
13 narcotics charges, searched the hotel room incident to the arrest, and seized a cache of stolen
14 travelers checks. *Id.* Thompson moved to suppress all evidence as the product of an illegal
15 search and seizure. *Id.* at 392. The trial judge denied the motion. *Id.* at 393. A divided panel
16 of the Ninth Circuit affirmed, finding that the marijuana was “accidentally exposed” and that
17 the police were not required to “close their eyes” to it. *Id.*

18 The government's argument is not persuasive. The holding in *Thompson* is an extension
19 of the plain-view doctrine. Police may seize incriminating evidence in plain view which they
20 come across inadvertently when they have a “prior justification” for the intrusion. *Coolidge v.*
21 *New Hampshire*, 403 U.S. 443, 466 (1971). That is to say, the police must be “lawfully
22 present” on the premises. *See Kyllo v. United States*, 533 U.S. 27, 38 (2001); *United States v.*
23 *Alfonso*, 759 F.2d 728, 743 (9th Cir. 1985). In *Thompson*, police were lawfully present in
24
25
26
27
28

1 Thompson's hotel room because Thompson had invited them in. *Thompson*, 382 F.2d at 393.
2 The officers did not snoop around while they were there. Auther, by contrast, had no legitimate
3 justification to intrude on anyone's conduct on the school laptop once it was no longer on loan
4 to his son. Moreover, the incriminating evidence did not drop out while he was straightening
5 the icons on the computer's desktop but came into view because of intentional spying on the
6 keyboard and hard drive.

7
8 Weindl argues that Auther's presence on the laptop through eBlaster was unlawful from
9 the start, because it violated PSS's laptop program agreement as well as the terms of his
10 eBlaster license. Because the Court finds that Auther was not acting under color of law when
11 he agreed to let his son use the PSS-issued laptop or when he purchased and installed eBlaster,
12 for purposes of this motion, it is irrelevant whether he breached these private contracts.

13
14 In summary, Auther's initial receipt and opening of eBlaster reports on Friday, June 15,
15 are not Fourth Amendment searches, but the receipt and opening of eBlaster reports on Monday,
16 June 18, are.

17
18 2. Whether Evidence Seized Through eBlaster Searches Must Be
19 Suppressed Under Federal Wiretap Statutes

20 The federal Wiretap Act, as amended by the Electronic Communications Privacy Act of
21 1986 and codified at 18 U.S.C. § 2510 *et seq.*, broadly prohibits interception of wire, oral, and
22 electronic communications except as expressly authorized. Statutory limitations on the use of
23 intercepted evidence apply "regardless of whether the interception was governmental or
24 private." *Chandler v. United States Army*, 125 F.3d 1296, 1298 (9th Cir. 1997).

25
26 The federal wiretap statute allows a private right of action to recover civil damages for
27 unlawful interception of wire, oral, or electronic communication. *See* 18 U.S.C. § 2520; *Klumb*
28

1 v. *Goan*, 2012 U.S. Dist. LEXIS 100836 (E.D. Tenn. July 19, 2012). In criminal prosecutions,
2 however, suppression motions are authorized only with respect to the contents of wire and oral
3 – not electronic – communications. *See* 18 U.S.C. § 2518(10); *United States v. Reed*, 575 F.3d
4 900, 915 (9th Cir. 2009). Clearly, the eBlaster e-mails are not “oral communication uttered by a
5 person . . .” 18 U.S.C. § 2510(2). The remaining question is whether they are wire
6 communications as defined by statute.
7

8 A wire communication is “any aural transfer” involving wire or like connections
9 between the point of origin and point of reception. 18 U.S.C. § 2510(1). An “aural transfer” is
10 “a transfer containing the human voice” at some point in transmission of the communication.
11 18 U.S.C. § 2510(18). There is no evidence that the transmission of information from the
12 school laptop to Auther via eBlaster entailed hearing a human voice. Therefore, the evidence
13 that Weindl seeks to suppress is not the product of a wire communication.
14

15 This result accords with the case law on spyware. In an early case, the “Miltan Spy
16 Function” recorded the requests made of a computer by an intruder as well as the computer’s
17 responses to the requests. *United States v. Seidlitz*, 589 F.2d 152, 154 (4th Cir. 1978). The
18 information recorded by the spyware was not subject to suppression, because there was “no
19 evidence to suggest that the ‘spy’ relied in any fashion upon sounds in retrieving information
20 from the computers in written form.” *Id.* at 157.
21

22 Weindl cites to no case where the results of spyware searches were suppressed. All his
23 citations involve civil suits for damages, which the statute authorizes for “electronic
24
25
26
27
28

communications.” They are not applicable in the criminal context. Therefore, any Wiretap Act violation because of Auther’s conduct does not merit suppression of evidence.⁵

3. Whether Weindl Has Fourth Amendment Standing

Although the post-June 15 eBlaster reports are the product of constitutionally protected searches of property, Weindl must show that he has standing to shield himself from them. To have standing to bring a Fourth Amendment claim arising from a search of property, a person must show a subjective expectation of privacy that is objectively reasonable. *United States v. Taketa*, 923 F.2d 665, 670 (9th Cir. 1991). Even if a person has “exhibited an actual (subjective) expectation of privacy” in his activities, he or she lacks Fourth Amendment standing if this expectation is not “one that society is prepared to recognize as ‘reasonable.’” *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)). A person “aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person’s premises or property has not had any of his Fourth Amendment rights infringed.” *Rakas v. Illinois*, 439 U.S. 128, 134 (1978) (quoted in *Taketa*, 923 F.2d at 670).

The laptop on which the alleged illicit activity was conducted did not belong to Weindl. It was purchased by PSS with the aid of a federal grant and issued to Auther’s son pursuant to PSS’s One on One Laptop Computer Policy. (See Ex. A.) The laptop, PSS says in its policy booklet, is the property of PSS. (See *id.* at 4 (“Ownership”).) In addition, Tim Thornburgh, the

⁵ Even if the remedy of suppression were available when evidence is gathered through unlawful interception of electronic communications, it is not clear that the eBlaster e-mails would qualify. At least one federal trial court has found that keystroke monitoring by spyware is not “electronic communication” as defined at 18 U.S.C. §2510(12) because it intercepts keystrokes during transmission *within* the computer, from keyboard to central processing unit, not by a system that affects interstate commerce. *United States v. Ropp*, 347 F. Supp. 2d 831, 837 (C.D. Cal. 2004). *Ropp* is a criminal case, but the issue was not presented in a suppression motion. *Ropp* was charged with attempting to intercept electronic communications, in violation of 18 U.S.C. §2511, by installing a device called KeyKatcher on someone else’s computer, and he moved to dismiss on grounds that the alleged conduct did not involve intercepting electronic communications. *Id.* at 831–32.

1 director of PSS's laptop program, testified that PSS owned the laptop and that PSS laptops were
2 distributed to students only. If the student graduates from high school, the student gets to keep
3 the laptop. If the student does not graduate, then the laptop is returned to the student's school
4 and redistributed to another student. None of the laptops are issued to any teachers or school
5 administrators.

6
7 In his Declaration, Weindl tries to establish a property interest in the laptop. He asserts
8 that "[f]or all extents [*sic*] and purposes, the laptops [in the program] belonged to Whispering
9 Palms School[.]" which was "solely responsible for inventorying and issuing the laptops" and
10 was "never required to account for the laptops to either the federal government or PSS." (First
11 Decl. ¶ 7.) Yet even if Whispering Palms had some claim to a property interest, on a theory that
12 the laptops were a gift or had been abandoned by PSS, that claim would not extend to Weindl.
13 Whispering Palms is a not-for-profit corporation (*id.* ¶ 7), not a privately owned business.
14 Corporate assets do not belong to the officers and directors. Weindl, even as president and sole
15 director of Whispering Palms, did not have a property interest in the laptop.
16

17
18 But that is not the end of the inquiry into Weindl's standing to challenge the search.
19 The capacity to bring a Fourth Amendment claim "depends not upon a property right in the
20 invaded place" but on privacy expectations. *Rakas*, 439 U.S. at 143. Weindl asserts he
21 expected his activities on the laptop to be private. He notes that the laptops carried no warning
22 that their use would not be private, and that laptop use was not monitored by Whispering Palms,
23 PSS, or the federal government. (First Decl. ¶ 8.) He declares that this past summer, he
24 operated a "school laptop" in his private, locked office for his sole personal use. (*Id.* ¶ 9.) He
25 states that he viewed his office as his "second home," and considered the office and the
26 computer he used to be private. (*Id.* ¶ 10.) He maintains that when not using the laptop, he
27
28

1 stored it in a desk drawer and never gave anyone “permission to use this laptop or remove it
2 from my office.” (*Id.* ¶ 12.)

3 Sometimes, people delude themselves into thinking that they have a right to things that
4 don’t belong to them. That appears to be the case here, with respect to Weindl’s use of school
5 laptops. The PSS laptops in the One to One laptop policy are intended for use by students, not
6 administrators and directors. The purpose of the policy is to “provide all students with a laptop
7 computer.” (Ex. A at 4.) To receive a laptop, students and a parent or guardian must sign an
8 agreement with PSS. (*Id.*) No evidence indicates that Weindl had a right to use, or himself had
9 permission to use, a PSS laptop, even for school-related activities. Auther turned his son’s
10 laptop in to Weindl in Weindl’s capacity as an agent for the school, not for Weindl’s personal
11 use.
12

13
14 Even if Weindl had a subjective (albeit unrealistic) expectation of privacy in the PSS
15 laptop, it was not an expectation that society is prepared to endorse. An expectation of privacy
16 does not become objectively reasonable just because a person hides someone else’s property
17 away in his office desk and does not let anyone else use it. A person cannot have a reasonable
18 expectation of privacy in a computer he stole or obtained by fraud. *See United States v. Wong*,
19 334 F.3d 831, 839 (9th Cir. 2003) (stolen laptop); *United States v. Caymen*, 404 F.3d 1196,
20 1201 (9th Cir. 2005) (fraudulently obtained laptop). In *Caymen*, police got a warrant to seize
21 from the defendant a laptop suspected to have been obtained through credit card fraud.
22 *Caymen*, 404 F.3d at 1197. After the seizure, they discovered that the defendant had a prior
23 conviction for possession of child pornography. *Id.* at 1198. They then conducted a warrantless
24 search of the laptop’s hard drive, ostensibly looking for evidence of credit card fraud, and
25 instead found sexually explicit images of children. *Id.* The defendant moved to suppress the
26
27
28

1 images, and the motion was denied on grounds that the defendant lacked Fourth Amendment
2 standing. *Id.* On appeal, the Ninth Circuit affirmed. It found that “one who takes property by
3 theft or fraud cannot reasonably expect to retain possession and exclude others from it once he
4 is caught. Whatever expectation of privacy he might assert is not a legitimate expectation that
5 society is prepared to honor.” *Id.* at 1201.

6
7 Weindl’s case is similar to *Wong* and *Caymen*. Weindl misappropriated school property
8 for his own personal use. Whatever expectation of privacy he developed in the contents of the
9 laptop’s hard drive and the keystrokes of Internet searches is not a legitimate one that society is
10 prepared to accept. This is different from the situation where a search is conducted of an
11 employee’s designated workplace computer, in which to some degree an employee has a
12 reasonable privacy expectation. *See, e.g., United States v. Ziegler*, 474 F.3d 1184, 1189–90 (9th
13 Cir. 2007). The laptop was not assigned to Weindl and was not his office computer. For these
14 reasons, Weindl lacks standing to claim a Fourth Amendment violation with respect to the
15 eBlaster reports.
16

17 **B. Suppression of Statements**

18
19 Weindl moves to suppress statements he made to Special Agents Ewing and Auther on
20 June 28, 2012, as the product of custodial interrogation without the benefit of *Miranda*
21 warnings. In *Miranda v. Arizona*, 384 U.S. 436 (1966), the Supreme Court adopted
22 prophylactic measures to protect against coerced, and hence unreliable, confessions. A person
23 in police custody must be advised that he has a right to remain silent and to have counsel
24 present during questioning. *Id.* at 444–45. These protections are “constitutional in nature.”
25 *United States v. Craighead*, 539 F.3d 1073, 1082 (9th Cir. 2008) (citing *Dickerson v. United*
26
27
28

1 *States*, 530 U.S. 428 (2000)). Any unwarned statements made during custodial interrogation are
2 not admissible at trial. *Miranda*, 384 U.S. at 476.

3 The parties do not dispute that Weindl was interrogated in his office and that he was not
4 advised of his rights before or during that questioning. The only issue is whether Weindl was in
5 custody at the time.

6
7 After the office interview, Weindl was formally placed in custody and given an advice
8 of rights form to sign. The government bears a heavy burden to demonstrate that a person in
9 custody knowingly and intelligently waived his or her right to remain silent and right to counsel
10 before making incriminating statements in response to police questioning. *See United States v.*
11 *Rodriguez*, 518 F.3d 1072, 1076 (9th Cir. 2008) (citing *Miranda*, 384 U.S. at 475). The validity
12 of the waiver depends on whether the totality of the circumstances shows that the defendant was
13 aware of the nature of his rights and the consequences of abandoning them. *See United States v.*
14 *Labrada-Bustamante*, 428 F.3d 1252, 1259 (9th Cir. 2005). If Weindl was did not voluntarily
15 waive his rights, any statements he made in response to FBI questioning while in the agents'
16 vehicle and during the search for the laptop's hard drive would be inadmissible.

17
18
19 1. Whether Weindl Was in Custody During the Office Interview

20 A person is in police custody if he has been formally arrested or "otherwise deprived of
21 his freedom of action in any significant way." *Miranda*, 384 U.S. at 444. *See also Berkemer v.*
22 *McCarty*, 468 U.S. 420, 440 (1984) (in custody when freedom of action is curtailed to a degree
23 associated with formal arrest). Informal custody is determined by examining "the totality of the
24 circumstances surrounding the interrogation." *Craighead*, 539 F.3d at 1082. The test is an
25 objective one: whether a "reasonable person in [defendant's] position" would have felt so
26 deprived of his freedom to act "that he would not have felt free to terminate the interrogation."
27
28

1 *Id.*; see also *United States v. Booth*, 669 F.2d 1231 (9th Cir. 1981) (defendant in custody if
2 “reasonable innocent person in such circumstances would conclude that after brief questioning
3 he or she would not be free to leave.”). Hallmarks of custody include “incommunicado
4 interrogation of individuals in a police-dominated atmosphere.” *Miranda*, 384 U.S. at 445.
5 Among the factors are “(1) the language used to summon the individual; (2) the extent to which
6 the defendant is confronted with evidence of guilt; (3) the physical surroundings of the
7 interrogation; (4) the duration of the detention; and (5) the degree of pressure applied to detain
8 the individual.” *United States v. Beraun-Panez*, 812 F.2d 578, 580 (9th Cir. 1987). When the
9 interrogation is conducted in “locations outside the police station,” such as a person’s home or
10 office, the proper approach is to consider “the extent to which the circumstances of the
11 interrogation turned the otherwise comfortable and familiar surroundings . . . into a ‘police-
12 dominated atmosphere.’” *Craighead*, 539 F.3d at 1083.

15 In this case, Weindl was not formally arrested until after the interview in his office at
16 Whispering Palms concluded. The FBI agents did not summon Weindl to speak with them
17 immediately but waited outside his office while he finished a conversation with someone else.
18 When that conversation ended, the agents engaged in social small talk with Weindl and the
19 other person outside. It is not clear whether it was Weindl or one of the agents who suggested
20 they move the interview inside. But it seems most likely that this was a joint decision motivated
21 by a combination of loud noise outdoors from a maintenance crew and the sensitive nature of
22 the agents’ questions. Courts have found interrogation to be noncustodial when the defendant
23 “agreed to accompany” officers to a room. *United States v. Bassignani*, 575 F.3d 879, 884 (9th
24 Cir. 2009) (citing *United States v. Crawford*, 372 F.3d 1048, 1059 (9th Cir. 2004); *United States*
25
26
27
28

1 v. *Norris*, 428 F.3d 907, 912 (9th Cir. 2005)). Weindl voluntarily agreed to speak with the
2 agents in his office.

3 The physical surroundings were not oppressive. Weindl and Auther had spoken together
4 in Weindl's office many times, about school matters. Although the office was small and narrow
5 and Auther's seat blocked the door to the outside, the circumstances show that Weindl had some
6 freedom of movement. At the start of the interview, the agents allowed Weindl to go into a
7 classroom, most likely through the inner door, to retrieve an extra chair. Moreover, Auther's
8 offer to leave the room so that Weindl and Ewing could talk privately conveyed the agents'
9 willingness to create as comfortable an environment as possible under the circumstances.
10

11 The length of the interview, between 45 minutes and one hour, does not tip the scales
12 toward or away from a determination of custody. A two-and-a-half-hour interrogation of a
13 suspect in a child pornography investigation was noncustodial where it was "conducted in an
14 open, friendly tone" and the suspect "participated actively." See *Bassignani*, 575 F.3d at 884.
15 In contrast, a mere 20–30 minute interrogation in another child pornography case was custodial
16 where it took place in a remote storage room of the suspect's house while other law
17 enforcement officers executed a search warrant. See *Craighead*, 539 F.3d at 1078, 1086–87.
18 The Court finds that other circumstances than the duration of the questioning are more helpful
19 to determining whether Weindl was in custody.
20

21 Over the course of the interview, Ewing repeatedly confronted Weindl with evidence of
22 his guilt. He encouraged Weindl to tell what happened to the laptop by showing him the
23 inconsistencies in his story, and by warning that the agents would have to start questioning
24 school parents and staff if Weindl did not help them. While these tactics were highly
25 persuasive, they were not unduly coercive. Any interview of a suspect by police "will have
26
27
28

1 coercive aspects to it,” but that alone does not make it a custodial situation. *Oregon v.*
2 *Mathiason*, 429 U.S. 492, 495 (1977) (per curiam).

3 As to the degree of pressure used to detain the suspect, Weindl was not handcuffed
4 during the interview or otherwise physically restrained. Although Ewing and Auther never told
5 Weindl he was free to leave, they never gave any indication he had to stay until he gave
6 satisfactory answers to their questions.
7

8 On balance of the five factors reviewed above, the Court finds that the circumstances of
9 the questioning of Weindl in his office do not indicate a police-dominated atmosphere, and that
10 the interrogation was noncustodial.

11 Other tests of informal custody yield the same result. In determining whether an
12 interview of a suspect at his home was custodial, the Ninth Circuit considered “(1) the number
13 of law enforcement personnel and whether they were armed; (2) whether the suspect was at any
14 point restrained, either by physical force or by threats; (3) whether the suspect was isolated from
15 others; and (4) whether the suspect was informed that he was free to leave or terminate the
16 interview, and the context in which any such statements were made.” *Craighead*, 539 F.3d at
17 1084. In *Craighead*, a case in which the Ninth Circuit found informal custody, eight law
18 enforcement officers from three separate agencies came to the suspect’s residence to execute a
19 search warrant for child pornography and to interview the suspect. *Id.* at 1078. All were armed
20 and wearing flak jackets; some unholstered their weapons in his presence. *Id.* The search was
21 conducted by some of the officers while others interviewed the suspect. *Id.* Officers directed
22 the suspect to a cluttered storage room at the back of the house for questioning. *Id.* The FBI
23 special agent who conducted the questioning wore a flak jacket and a sidearm. *Id.* Although
24 the FBI special agent had told the suspect he was free to terminate the interview and would not
25
26
27
28

1 be arrested that day, the suspect testified that he felt he was not free to leave, that he knew
2 several officers from two other law enforcement agencies were searching his house, and that he
3 was uncertain that they, as opposed to the FBI, would allow him to leave. *Id.* at 1079.

4 In Weindl's case, only two law enforcement officers were present before and during the
5 interview; there were plenty of "police-free rooms or spaces to which the suspect may [have]
6 retreat[ed]" had he wished to terminate the interview. *Id.* at 1085. No weapons were visible, let
7 alone drawn. Weindl was not handcuffed or otherwise physically restrained or threatened.
8 Although the interview took place in a private office and access to the outside door was
9 blocked, it cannot be said that Weindl was isolated. The office was centrally located within the
10 school building. Most of all, this was Weindl's own office, where at any moment someone may
11 have come knocking on the door looking for him or calling him on the telephone. He was not
12 held incommunicado.

15 In a sworn declaration, Weindl stated that he did not consider Auther and Ewing's visit
16 to be "friendly"; that he had to cut short a meeting with another person in order to speak with
17 them; that the configuration of his small office and the blocking of the outside door made him
18 "feel cornered"; that he perceived Special Agent Ewing's repeated recitations of the evidence
19 against him, and warnings that a formal investigation would have to be launched if he did not
20 cooperate, to be "quite threatening and frightening"; and that he had the impression he was
21 going to be arrested if he did not answer their questions, and did not feel free to refuse. (*See*
22 *First Decl.* ¶¶ 13–21.)

25 In weighing the credibility of Weindl's two sworn declarations, the Court takes into
26 account that because Weindl did not testify at the hearing, his statements have not been "test[ed]

1 in the crucible of cross-examination.” *Crawford v. Washington*, 541 U.S. 36, 61 (2004).⁶ Yet
2 even if Weindl’s description of his subjective state of mind were to be fully credited, it does not
3 establish that a reasonable person in his situation would not have felt free to terminate the
4 interview. It is not enough that Weindl knew that Ewing and Auther suspected him of accessing
5 child pornography. The objective circumstances of the questioning must be so oppressive as to
6 establish that the restraint of the suspect’s freedom of movement was “of the degree associated
7 with formal arrest.” *See Stansbury v. California*, 511 U.S. 318, 322 (1994). In *Craighead*, the
8 interview took place in the midst of an armed raid on the suspect’s home. Weindl, in contrast,
9 was not aware that other officers were present at the school until after the interview ended and
10 he came out of the office. Moreover, he was not even informed of the existence of a search
11 warrant until after the interview. The totality of the circumstances of the interview do not
12 amount to informal custody.
13
14

15 2. Whether Weindl’s Waiver of Rights Was Effective

16 The only remaining question is whether Weindl effectively waived his *Miranda* rights
17 after he was taken into custody following the interview. Ewing testified that he handed Weindl
18 a standard FBI advice of rights form to read and sign at the picnic tables. He said he told
19 Weindl that he was not going to read the rights aloud to him unless Weindl needed him to, so as
20 not to call public attention to the fact that Weindl was being arrested. He testified that after
21 Weindl had a chance to read the form, he asked Weindl if he understood it, and Weindl said he
22 did. Weindl signed the form at the bottom, as witnessed by Ewing and another agent. (See Ex.
23 3.) He did not place his initials next to any of the six listed rights. Weindl maintains that he
24
25
26

27 ⁶ A defendant’s testimony on a motion to suppress, in order to vindicate his rights under the Fourth Amendment,
28 does not waive his Fifth Amendment right to remain silent and cannot be used against him at trial to establish his
guilt. *See Simmons v. United States*, 390 U.S. 377, 390 (1968). However, it may be used to impeach him at trial if
he testifies on his own behalf. *See United States v. Beltran-Gutierrez*, 19 F.3d 1287, 1289 (9th Cir. 1994).

1 was “told to sign a piece of paper” but “I did not read it carefully because I was upset.” (First
2 Decl. ¶ 21.)

3 On the one hand, it is clear both from his chosen profession and by his written
4 declarations that Weindl is a well-educated person who has no difficulty reading and
5 understanding English. Although no doubt Weindl was upset at this point, he does not deny that
6 he read the form, only that he read it “carefully.”
7

8 On the other hand, it is troubling that the agents did not read Weindl his rights out loud
9 or get explicit confirmation that he understood each of the six rights listed on the form. If the
10 agents wanted to protect Weindl’s privacy, they could have taken him back into his office and
11 gone over his rights carefully with him there. Between the office interview and the formal
12 arrest, not once did an agent tell Weindl that he had the right to remain silent, that any
13 incriminating statements he made would be used against him, that he had a right to consult with
14 a lawyer and have a lawyer present during questioning, and a right to stop answering questions
15 at any time.
16
17

18 Although there is no precise form in which the *Miranda* rights need be given, it must be
19 sufficient to ensure that the defendant is “informed in clear and unequivocal terms” of his
20 constitutional rights. *Miranda*, 384 U.S. at 467–68. The defendant’s prior awareness of his
21 rights, because of his education or intelligence, does not shift the burden away from the
22 government. *See id.* at 471–72 (“[n]o amount of circumstantial evidence that the person may
23 have been aware of this right will suffice to stand” instead of adequate warning); *see also*
24 *United States v. Bland*, 908 F.2d 471, 474 n.1 (9th Cir. 1990) (rejecting government’s
25 suggestion that a defendant with prior experience with criminal justice system does not need
26 complete advisement of rights). This is because “whatever the background of the person
27
28

1 interrogated, a warning at the time of the interrogation is indispensable to overcome its
2 pressures and to insure that the individual knows he is free to exercise the privilege at that point
3 in time.” *Miranda*, 384 U.S. at 469.

4 The Court finds that the Government has not met its heavy burden to show that Weindl
5 made a knowing and intelligent waiver of his constitutional rights. Any statements made after
6 Weindl was placed in custody, and any evidence relating to or resulting from such statements,
7 may not be offered in the Government’s case in chief.

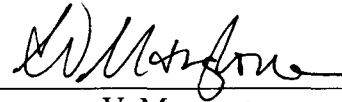
9 IV. CONCLUSION

10 The information contained in the eBlaster reports sent to Auther on June 15, 2012, is not
11 the product of a Fourth Amendment search. The information contained in the June 18 eBlaster
12 reports is the product of a constitutionally protected search, but Weindl does not have Fourth
13 Amendment standing to challenge the search. The federal wiretap statute does not provide for
14 suppression of data gathered by eBlaster because the contents of wire or oral communications
15 are not involved. For those reasons, the motion to suppress information in the eBlaster e-mails
16 and reports is DENIED.

17
18
19 Because the interrogation of Weindl by FBI special agents in his office at Whispering
20 Palms School on June 28, 2012, was noncustodial, the agents were not required to advise
21 Weindl of his constitutional rights before questioning him. Weindl’s statements in the office on
22 that date were voluntary and are admissible. However, any statements made after he was placed
23 in custody at the picnic tables, and the evidentiary fruits of those statements, are excluded from
24 the Government’s case in chief because Weindl was not adequately advised of his rights.
25 Therefore, the motion to suppress statements is DENIED IN PART AND GRANTED IN
26 PART.
27
28

1 The suppression motion having been denied in substantial part, there are insufficient
2 grounds to support the motion to dismiss, and it is DENIED.

3 SO ORDERED this 20th day of November, 2012.
4

5 

6 RAMONA V. MANGLONA
7 Chief Judge
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28