

**FOR PUBLICATION**  
**UNITED STATES COURT OF APPEALS**  
**FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA,  
*Plaintiff-Appellee,*  
v.  
MARK STEPHEN FORRESTER,  
*Defendant-Appellant.*

No. 05-50410  
D.C. No.  
CR-01-03177-TJW

UNITED STATES OF AMERICA,  
*Plaintiff-Appellee,*  
v.  
DENNIS LOUIS ALBA,  
*Defendant-Appellant.*

No. 05-50493  
D.C. No.  
CR-01-03177-1-  
TJW  
ORDER  
AMENDING  
OPINION AND  
DENYING  
PETITION FOR  
REHEARING AND  
SUGGESTION  
FOR REHEARING  
EN BANC AND  
AMENDED  
OPINION

Appeal from the United States District Court  
for the Southern District of California  
Thomas J. Whelan, District Judge, Presiding

Argued and Submitted  
January 12, 2007—Pasadena, California

Filed July 6, 2007  
Amended July 25, 2007  
Second Amendment January 7, 2008

Before: Raymond C. Fisher, Richard R. Clifton and  
Milan D. Smith, Jr., Circuit Judges.

Opinion by Judge Fisher

---

**COUNSEL**

Benjamin L. Coleman, Coleman & Balogh LLP, San Diego, California, for defendant-appellant Forrester.

Michael L. Crowley, San Diego, California, for defendant-appellant Alba.

Todd W. Robinson, Assistant United States Attorney, San Diego, California, for the plaintiff-appellee.

---

**ORDER**

The amended opinion filed July 25, 2007, at slip opinion 9045-9066, 495 F.3d 1041 (9th Cir. 2007), is amended as follows:

At slip op. 9059, second full paragraph, line 5: change the sentence beginning “We conclude that these surveillance techniques are constitutionally indistinguishable . . .” to “We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable . . .”.

At slip op. 9060, continuation paragraph, line 8: change the last two sentences in their entirety, beginning with “Analogously . . .” and ending with “. . . *Id.* at 744.” to “Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the “switching equipment that processed those numbers,” e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party’s servers. *Id.* at 744.”.

At slip op. 9060, first full paragraph: change the paragraph beginning with “Second, e-mail to/from addresses . . .” and ending at slip op. 9061 with “. . . enable only the discovery of addressing information.”<sup>6</sup> to: “Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person’s e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses — but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.”<sup>6</sup>.

---

<sup>6</sup>Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators (“URL”) of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person’s Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times’ website at <http://www.nytimes.com>, whereas a tech-

At slip op. 9065, second full paragraph, line 6: change the sentence beginning “We also hold that the government’s monitoring . . . Fourth Amendment purposes and that, . . .” to “We also hold that the techniques the government used to monitor Alba’s e-mail and Internet activity did not constitute a search for Fourth Amendment purposes and that, . . .”.

The mandate shall issue immediately in *United States v. Forrester*, No. 05-50410.

The parties in *United States v. Alba*, No. 05-50493, may file a petition for rehearing based on the amended opinion.

With these amendments the panel has voted to deny Appellant Alba’s petition for rehearing and suggestion for rehearing en banc.

The full court has been advised of the suggestion for rehearing en banc and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35.

Appellant Alba’s petition for rehearing and suggestion for rehearing en banc, filed August 21, 2007, is **DENIED**.

---

## OPINION

FISHER, Circuit Judge:

Defendants-appellants Mark Stephen Forrester and Dennis Louis Alba were charged with various offenses relating to the

---

nique that captures URLs would also divulge the particular articles the person viewed. *See Pen Register Application*, 396 F. Supp. 2d at 49 (“[I]f the user then enters a search phrase [in the Google search engine], that search phrase would appear in the URL after the first forward slash. This would reveal content . . .”).

operation of a large Ecstasy-manufacturing laboratory, and were convicted on all counts following a jury trial. They now appeal their convictions and sentences.

Forrester moved to represent himself prior to trial. At the hearing on this motion, the district court carefully warned Forrester of the dangers of self-representation, but did not inform him of the charge against him and told him that he faced 10 years to life in prison whereas he actually faced a potential prison term of zero to 20 years. The omission and the misstatement compel us to hold that Forrester's waiver of his right to counsel was not knowing and intelligent and that the Sixth Amendment was violated when he was allowed to proceed pro se. Accordingly, we reverse Forrester's conviction and sentence.

Alba challenges the validity of computer surveillance that enabled the government to learn the to/from addresses of his e mail messages, the Internet protocol ("IP") addresses of the websites that he visited and the total volume of information transmitted to or from his account. We conclude that this surveillance was analogous to the use of a pen register that the Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), did not constitute a search for Fourth Amendment purposes. Moreover, whether or not the surveillance came within the scope of the then-applicable federal pen register statute, Alba is not entitled to the suppression of the evidence obtained through the surveillance because there is no statutory or other authority for such a remedy.<sup>1</sup>

---

<sup>1</sup>Alba's remaining arguments are addressed in a concurrently filed memorandum disposition. As requested by the parties, we vacate his conviction and sentence for conspiracy to manufacture and distribute Ecstasy. We otherwise affirm Alba's convictions and sentences, but reduce his supervised release term from six to five years.

---

## I. BACKGROUND

Following a lengthy government investigation, Forrester and Alba were indicted on October 26, 2001, and arraigned shortly thereafter. Forrester was charged with one count of conspiracy to manufacture and distribute 3, 4-methylenedioxymethamphetamine (“Ecstasy”) in violation of 21 U.S.C. §§ 841(a)(1), 846. Alba was also charged with that offense, as well as with engaging in a continuing criminal enterprise in violation of 21 U.S.C. § 848(a), conspiracy to transfer funds outside the United States in promotion of an illegal activity in violation of 18 U.S.C. § 1956(a)(2)(A)(i), (h) and conspiracy to conduct financial transactions involving the proceeds of an illegal activity in violation of 18 U.S.C. § 1956(a)(1)(A)(i), (h). Both defendants pleaded not guilty to all charges.

Forrester is represented by counsel on appeal. He also had legal representation from the time his indictment was filed until October 23, 2002, when the district court heard and granted his motion to represent himself, as well as during some of the post-trial proceedings. At the October 23 hearing, the court repeatedly warned Forrester that defendants who represent themselves rarely succeed. The court said to Forrester, for example, “I want to unequivocally tell you and strongly recommend to you that you don’t do this. In most cases it’s a disaster,” and “in all cases it is not a good idea for a nonlawyer to oppose a lawyer in a criminal trial.” Forrester, in turn, repeatedly assured the court that he understood the implications of his decision and wished to proceed pro se. He told the court that he was “aware of the consequences” and that “I’m coherent and I’m literate and I understand what my consequences are.” Unfortunately, the court did not apprise Forrester of the charge against him at the hearing, and gave him incorrect information about the potential sentence that he faced. The court said that he faced “a mandatory minimum of ten years in jail and possibly up to life.” In fact, Forrester

faced no mandatory minimum and a maximum of 20 years in prison.<sup>2</sup>

The district court held a follow-up hearing on March 7, 2003 to find out how Forrester was coping with self-representation. The court confirmed that Forrester had access to discovery materials, instructed him to be more timely with his motions and rejected his request for the appointment of a new standby attorney. However, the court again did not inform Forrester of the charge against him, nor did it correct its error about his potential sentence. The court's omission and misstatement were not corrected at any other point before trial.

During its investigation of Forrester and Alba's Ecstasy-manufacturing operation, the government employed various computer surveillance techniques to monitor Alba's e-mail and Internet activity. The surveillance began in May 2001 after the government applied for and received court permission to install a pen register analogue known as a "mirror port" on Alba's account with PacBell Internet. The mirror port was installed at PacBell's connection facility in San Diego, and enabled the government to learn the to/from addresses of Alba's e-mail messages, the IP addresses of the websites that Alba visited and the total volume of information sent to or from his account. Later, the government obtained a warrant authorizing it to employ imaging and keystroke monitoring techniques, but Alba does not challenge on appeal those techniques' legality or the government's application to use them.

Forrester and Alba were tried by jury. At trial, the government introduced extensive evidence showing that they and their associates built and operated a major Ecstasy laboratory.

---

<sup>2</sup>The maximum was increased to 30 years when, just before trial, the government filed an information informing the court of Forrester's prior felony drug convictions.



Witnesses described the lab as “very, very large,” and seized documents show that it was intended to produce approximately 440 kilograms of Ecstasy (and \$10 million in profit) per month. The government also presented evidence that Alba purchased precursor chemicals for Ecstasy, that Forrester met with a Swedish chemist in Stockholm to learn about manufacturing Ecstasy, that the defendants first tried to construct the lab in two other locations before settling on Escondido, California and that the Escondido lab was located inside an insulated sea/land container and contained an array of devices and chemicals used to make Ecstasy.

The jury convicted Forrester and Alba on all counts. The district court sentenced them each to 360 months in prison and six years of supervised release. Both defendants timely appealed.

## II. STANDARD OF REVIEW

The validity of a waiver of the right to counsel is reviewed de novo. *United States v. Erskine*, 355 F.3d 1161, 1166 (9th Cir. 2004). Conclusions of law underlying the denial of a motion to suppress evidence are also reviewed de novo. *United States v. Vesikuru*, 314 F.3d 1116, 1119 (9th Cir. 2002).

## III. DISCUSSION

### A. Waiver of the Right to Counsel

Forrester argues that his waiver of the right to counsel at the October 23, 2002 hearing was not knowing and intelligent because the district court failed to inform him of the charge against him and misinformed him about the potential sentence he faced. As a result, Forrester contends, his conviction and sentence must be reversed. We agree with Forrester as to both the constitutional violation and the requisite remedy.

[1] *Faretta v. California*, 422 U.S. 806 (1975), held that a defendant has a constitutional right to represent himself but that “the accused must knowingly and intelligently forgo those relinquished benefits. . . . [H]e should be made aware of the dangers and disadvantages of self-representation, so that the record will establish that he knows what he is doing and his choice is made with eyes open.” *Id.* at 835 (internal quotations omitted). This court has gleaned a three-factor test from *Faretta*, under which “[i]n order to deem a defendant’s *Faretta* waiver knowing and intelligent, the district court must insure that he understands 1) the nature of the charges against him, 2) the possible penalties, and 3) the ‘dangers and disadvantages of self-representation.’ ” *Erskine*, 355 F.3d at 1167 (quoting *United States v. Balough*, 820 F.2d 1485, 1487 (9th Cir. 1987)). On appeal, the burden of establishing the legality of the waiver is on the government, *id.*, and “courts indulge in every reasonable presumption against waiver,” *United States v. Arlt*, 41 F.3d 516, 520-21 (9th Cir. 1994) (quoting *Brewer v. Williams*, 430 U.S. 387, 404 (1977)). *See also United States v. Mohawk*, 20 F.3d 1480, 1484 (9th Cir. 1994) (describing the government’s burden as “a heavy one”). Ordinarily, only the defendant’s colloquy with the court at the *Faretta* hearing is relevant to the waiver analysis. *Id.* However, a “limited exception” exists whereby “a district court’s failure to discuss each of the elements in open court will not necessitate automatic reversal when the record as a whole reveals a knowing and intelligent waiver.” *Balough*, 820 F.2d at 1488.

[2] Here the district court clearly apprised Forrester of the “dangers and disadvantages of self-representation” at the *Faretta* hearing. It “unequivocally” and “strongly” recommended against waiving his right to counsel, told him that “[i]n most cases it’s a disaster” and described in detail the many unfamiliar tasks he would have to carry out if he took charge of his own defense. However, the district court failed to advise Forrester of the “nature of the charge[ ] against him.” *Erskine*, 355 F.3d at 1167. There is no mention of the

conspiracy charge in the hearing transcript, let alone any indication that the court sought to ensure that Forrester understood the charge and grasped that conspiracy is a particularly complex and confusing allegation to defend against. Furthermore, the district court did not accurately describe the “possible penalties” faced by Forrester. *Id.* The court told him that he faced 10 years to life in prison, whereas he actually faced the materially different sentence range of zero to 20 years in prison.

[3] On this record, the government cannot meet its burden of showing that Forrester’s waiver of the right to counsel was knowing and intelligent — especially given our case law that the government has a heavy burden and that we must indulge in all reasonable presumptions against waiver. *See Arlt*, 41 F.3d at 520; *Mohawk*, 20 F.3d at 1484. Of course, Forrester *may* have correctly understood the charge against him and the potential penalties, but the government has failed to *prove* that he did so. There is simply no evidence in the *Faretta* hearing transcript, which is ordinarily the only part of the record to which we look, that Forrester was informed of or comprehended the charge and penalties. *See Mohawk*, 20 F.3d at 1485 (“We think Mohawk’s decision to waive his right to counsel may well have been knowing and intelligent — but we are not free from doubt. . . . We therefore hold that the government has failed to carry its burden . . . .”); *United States v. Crowhurst*, 596 F.2d 389, 390 (9th Cir. 1979) (per curiam) (“[A]n accused individual must specifically be made aware of the charges and their possible penalties and sanctions.”).

[4] The government argues that there was no Sixth Amendment violation because the district court *overstated* the penalties that Forrester faced. According to the government, a defendant’s right to counsel is not thereby violated because he would have been *more* likely to waive that right had he known the actual, lower penalties he faced. The first flaw in this argument — which the government fails to support with

any legal authority — is that it is not clear how a defendant’s decision to waive his right to counsel may be affected by incorrect information about his potential sentence. It may be, as in *Erskine*, that a defendant is more likely to waive his right to counsel when he is told the stakes are lower than they actually are. On the other hand, as Forrester contends, it may be that a middle-aged defendant is more prone to roll the dice with self-representation when he distrusts his lawyer and is told that, no matter what he does, he will be in jail for at least a decade if he is convicted. Had Forrester known that the stakes were lower and that he faced no mandatory minimum sentence, he may have been more likely to keep his attorney despite his misgivings about the attorney’s skill and commitment to his case. *Cf. United States v. Stubbs*, 279 F.3d 402, 411 (6th Cir. 2002) (“When the maximum possible sentence exposure is overstated, the defendant might well be influenced to accept a plea agreement he would otherwise reject.”) (internal quotation marks omitted). The causal connection the government suggests exists between information about one’s potential sentence and waiver of the right to counsel may be plausible, but it is far from inevitable.

[5] The second problem with the government’s sentence overstatement argument is that it is in essence a harmless error claim. The government contends, though not in so many words, that even though Forrester was unaware of the actual penalty he faced, there was no harm because he would have waived counsel even if he had been properly informed. But this court has repeatedly rejected harmless error analysis in the *Faretta* waiver context. *See Erskine*, 355 F.3d at 1167 (“[T]he failure to meet the requirements for a valid *Faretta* waiver constitutes per se prejudicial error, and the harmless error standard is inapplicable.”); *Mohawk*, 20 F.3d at 1484 (invalid *Faretta* waiver “requires automatic reversal of a defendant’s conviction”); *Balough*, 820 F.2d at 1490; *cf. McKaskle v. Wiggins*, 465 U.S. 168, 177 n.8 (1984) (“Since the right of self-representation is a right that when exercised usually increases the likelihood of a trial outcome unfavorable

to the defendant, its denial is not amenable to ‘harmless error’ analysis.”). It is thus irrelevant whether the district court overstated or understated Forrester’s potential penalty. By materially misstating the applicable sentence, the court failed to fulfill its obligation to “insure that [the defendant] understands . . . the possible penalties,” and Forrester’s waiver was therefore not knowing and intelligent. *Erskine*, 355 F.3d at 1167.<sup>3</sup>

The government also invokes the “limited exception” that allows courts to consider the record as a whole rather than solely the *Faretta* hearing transcript when determining the validity of a waiver. See *Balough*, 820 F.2d at 1488. However, this limited exception is meant to be applied only in “rare cases.” *United States v. Harris*, 683 F.2d 322, 324 (9th Cir. 1982); see also *United States v. Rylander*, 714 F.2d 996, 1005 (9th Cir. 1983) (“It is an unusual case where, absent [a proper] colloquy, a knowing and intelligent waiver of counsel will be found.”). In addition, Forrester’s active involvement in his own defense, although probative, is insufficient to show that his waiver of the right to counsel was knowing and intelligent. See *Balough*, 820 F.3d at 1489 (“[T]he mere fact that a criminal defendant has been repeatedly exposed to the legal process and has even represented himself before cannot, without more, suffice to support a finding of a knowing and intelligent waiver.”). Finally, the government, both in its briefing and at oral argument, was unable to point to any evidence in the record that concretely establishes Forrester’s understand-

---

<sup>3</sup>Moreover, even if the Sixth Amendment were not violated when a district court materially overstates a defendant’s potential sentence at a *Faretta* hearing, there is still the issue of the conspiracy charge against Forrester, whose nature the district court did not explain to Forrester at the hearing or anywhere else in the record. See *United States v. Dujanovic*, 486 F.2d 182, 186 (9th Cir. 1973) (“We cannot visualize a less minimal requirement than the District Court shall not grant a request to waive counsel . . . without . . . determining on the record that the demand to waive counsel . . . is competently and intelligently made with understanding of the nature of the charge . . .”).

ing of the charge against him and potential penalties, nor have we been able to locate any. Notably, Forrester was not specifically informed that he was being charged with conspiracy to manufacture and distribute Ecstasy at any of the three arraignments at which he was present; nor, at the March 7, 2003 follow-up hearing, did the district court correct its error as to Forrester's potential sentence or discuss the charge against him.

[6] We therefore hold that Forrester's waiver of the right to counsel was not knowing and intelligent and that the Sixth Amendment was violated as a result. Because harmless error analysis does not apply in this context, we have no choice but to reverse Forrester's conviction and sentence. *Cf. United States v. Keen*, 96 F.3d 425, 429-30 (9th Cir. 1996) ("Regrettably, given the overwhelming evidence of Keen's guilt and the inconvenience a retrial would impose . . . this discussion appears insufficient. . . . [He] is entitled to a reversal and an opportunity to make an informed and knowing choice.").

## **B. Computer Surveillance**

Alba contends that the government's surveillance of his e-mail and Internet activity violated the Fourth Amendment and fell outside the scope of the then-applicable federal pen register statute.<sup>4</sup> We hold that the surveillance did not constitute a

---

<sup>4</sup>As mentioned earlier, Alba complains only about the initial surveillance through which the government obtained the to/from addresses of his e-mail messages, the IP addresses of the websites that he visited and the total volume of information sent to or from his account. He does not challenge the more intrusive imaging and keystroke monitoring that subsequently took place (though he does argue that the information obtained through those techniques should be suppressed as tainted derivative evidence).

Alba did not explicitly move to suppress evidence obtained through the computer surveillance before the district court. However, both parties have

Fourth Amendment search and thus was not unconstitutional. We also hold that whether or not the computer surveillance was covered by the then-applicable pen register statute — an issue that we do not decide — Alba is not entitled to the suppression of any evidence (let alone the reversal of his convictions) as a consequence.

### 1. The Fourth Amendment

[7] The Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), that the use of a pen register (a device that records numbers dialed from a phone line) does not constitute a search for Fourth Amendment purposes. *Id.* at 745-46. According to the Court, people do not have a subjective expectation of privacy in numbers that they dial because they “realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.” *Id.* at 742. Even if there were such a subjective expectation, it would not be one that society is prepared to recognize as reasonable because “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Id.* at 743-44. Therefore the use of a pen register is not a Fourth Amendment search. Importantly, the Court distinguished pen registers from more intrusive surveillance techniques on the ground that “pen registers do not acquire the *contents* of communications” but rather obtain only the addressing information associated with phone calls. *Id.* at 741; *see also id.* at 743 (“Although petitioner’s conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated

---

briefed the constitutional and statutory issues raised by the surveillance, and the government does not contend that Alba has waived his Fourth Amendment and statutory claims. *See Tokatly v. Ashcroft*, 371 F.3d 613, 618 (9th Cir. 2004) (“[I]t is well-established that the government can ‘waive waiver’ implicitly by failing to assert it.”) (internal quotation omitted).

to preserve the privacy of the number he dialed.”); *cf. Katz v. United States*, 389 U.S. 347 (1967) (legitimate expectation of privacy exists in contents of phone conversation).

[8] Neither this nor any other circuit has spoken to the constitutionality of computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account.<sup>5</sup> We conclude that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*. First, e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication. *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users’ imputed knowledge that their calls are completed through telephone company switching equipment. 442 U.S. at 742. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Like telephone numbers, which provide instructions to the “switching equipment that processed those numbers,” e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party’s servers. *Id.* at 744.

---

<sup>5</sup>Every computer or server connected to the Internet has a unique IP address. A website typically has only one IP address even though it may contain hundreds or thousands of pages. For example, Google’s IP address is 209.85.129.104 and the New York Times’ website’s IP address is 199.239.137.200. See *In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxx@xxx.com]*, 396 F. Supp. 2d 45, 48 (D. Mass. 2005) (“*Pen Register Application*”) (citing government application that defined “IP address” as a “‘unique numerical address identifying each computer on the [I]nternet’ ”).



[9] Second, e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers. When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the e-mail to/from addresses and IP addresses — but this is no different from speculation about the contents of a phone conversation on the basis of the identity of the person or entity that was dialed. Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.<sup>6</sup>

---

<sup>6</sup>Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators (“URL”) of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at <http://www.nytimes.com>, whereas a technique that captures URLs would also divulge the particular articles the person viewed. See *Pen Register Application*, 396 F. Supp. 2d at 49 (“[I]f the user then enters a search phrase [in the Google search engine], that search phrase would appear in the URL after the first forward slash. This would reveal content . . .”).

[10] The government’s surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail. In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties. See *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (stating that warrantless searches of letters and sealed packages are “presumptively unreasonable”); *United States v. Van Leeuwen*, 397 U.S. 249, 251-52 (1970) (mail is “free from inspection . . . except in the manner provided by the Fourth Amendment,” but postal authorities could nonetheless detain mail without warrant based on suspicious appearance and circumstances); *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (“Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.”); see also *United States v. Hernandez*, 313 F.3d 1206, 1209-10 (9th Cir. 2002) (“Although a person has a legitimate interest that a mailed package will not be opened and searched en route, there can be no reasonable expectation that postal service employees will not handle the package or that they will not view its exterior.”) (internal citation omitted). E-mail, like physical mail, has an outside address “visible” to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not.

Finally, the pen register in *Smith* was able to disclose not only the phone numbers dialed but also the number of calls made. There is no difference of constitutional magnitude between this aspect of the pen register and the government’s

monitoring here of the total volume of data transmitted to or from Alba's account. Devices that obtain addressing information also inevitably reveal the amount of information coming and going, and do not thereby breach the line between mere addressing and more content-rich information.

[11] We therefore hold that the computer surveillance techniques that Alba challenges are not Fourth Amendment searches. However, our holding extends only to these particular techniques and does not imply that more intrusive techniques or techniques that reveal more content information are also constitutionally identical to the use of a pen register.

## 2. The Then-Applicable Pen Register Statute

Alba claims that the government's computer surveillance was not only unconstitutional but also beyond the scope of the then-applicable pen register statute, 18 U.S.C. § 3121-27 (amended October 2001).<sup>7</sup> Under both the old and new versions of 18 U.S.C. § 3122, the government must apply for and obtain a court order before it can install and use a pen register. When the surveillance at issue here took place in May-July 2001, the applicable statute defined a pen register as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3). Notwithstanding the government's invocation of this provision and application for and receipt of a court order, Alba maintains that the computer surveillance at issue here did not come within the statutory definition of a "pen register."

[12] Even assuming that Alba is correct in this contention, he would not be entitled to the suppression of the evidence obtained through the computer surveillance. As both the

---

<sup>7</sup>Unless otherwise noted, all citations are to the pre-October 2001 version of the pen register statute.

Supreme Court and this court have emphasized, suppression is a disfavored remedy, imposed only where its deterrence benefits outweigh its substantial social costs or (outside the constitutional context) where it is clearly contemplated by the relevant statute. *See, e.g., Hudson v. Michigan*, 126 S. Ct. 2159, 2163 (2006) (“Suppression of evidence . . . has always been our last resort, not our first impulse.”); *United States v. Lombera-Camorlinga*, 206 F.3d 882, 887 (9th Cir. 2000) (en banc) (citing “the infrequency with which we have allowed an exclusionary remedy for a non-constitutional harm”). Alba does not point to any statutory language requiring suppression when computer surveillance that is similar but not technically equivalent to a pen register is carried out. Indeed, he does not even identify what law or regulation the government may have violated if its surveillance did not come within the scope of the then-applicable pen register statute. The suppression of evidence under these circumstances is plainly inappropriate.

Our conclusion is bolstered by the fact that suppression still would not be appropriate even if the computer surveillance was covered by the pen register statute. Assuming the surveillance violated the statute, there is no mention of suppression of evidence in the statutory text. *Cf. id.* at 883-84 (holding that suppression of evidence was not an appropriate remedy for a violation of Article 36 of the Vienna Convention when nothing in the text of the treaty suggested such a remedy). Instead, the only penalty specified is that “[w]hoever knowingly violates subsection (a)” by installing or using a pen register without first obtaining a court order “shall be fined under this title or imprisoned not more than one year, or both.” 18 U.S.C. § 3121(d). Where the legislature has already specified a remedy for a statutory violation, here fines and imprisonment, “we would ‘encroach upon the prerogatives’ of Congress were we to authorize a remedy not provided for by statute.” *United States v. Frazin*, 780 F.2d 1461, 1466 (9th Cir. 1986) (quoting *United States v. Chanen*, 549 F.2d 1306, 1313 (9th Cir. 1977)).

[13] Indeed, two circuits have explicitly held (and we have implied) that evidence obtained in violation of the pen register statute need not be suppressed. See *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995) (“[T]he statutory scheme [of the pen register statute] does not mandate exclusion of evidence for violations of the statutory requirements.”); *United States v. Thompson*, 936 F.2d 1249, 1249-50 (11th Cir. 1991) (“We hold that information obtained from a pen register placed on a telephone can be used as evidence in a criminal trial even if the court order authorizing its installation does not comply with the statutory requirements.”); cf. *United States v. Butz*, 982 F.2d 1378, 1383 (9th Cir. 1993) (refusing to suppress evidence obtained in violation of state pen register statute). The statutory text, our general reluctance to require suppression in the absence of statutory authorization, other circuits’ holdings and our own indirect precedent all therefore lead us to conclude that suppression is inappropriate even if the computer surveillance came within the scope of the then-applicable pen register statute.

Finally, even if suppression were a valid remedy, any error in not excluding evidence was harmless. The evidence obtained through the computer surveillance was never introduced at trial and was used only as a minor portion of the government’s application for a court order authorizing imaging and keystroke monitoring. There was more than enough other evidence in that application to generate probable cause even if the to/from addresses of Alba’s e-mails, the IP addresses he accessed and the volume of data transmitted to or from his account had been suppressed. The discussion of the computer surveillance spanned only four pages of the 45-page supporting affidavit for the application, and revealed only that Alba had sent e-mails to Forrester and accessed certain chemicals websites. The remainder of the affidavit included extensive — and more incriminating — evidence obtained through physical surveillance, conventional pen registers, wiretaps and cooperating witness statements. Much of this other evidence predated the start of the computer surveil-

lance, and there is no indication that evidence obtained through the computer surveillance was used to obtain authorization for any of the other surveillance techniques discussed in the affidavit. *See Nix v. Williams*, 467 U.S. 431, 443-44 (1984) (warrant based in part on tainted evidence still valid if there were independent sources that created probable cause).

#### IV. CONCLUSION

We reverse Forrester's conviction and sentence because his waiver of the right to counsel was not knowing and intelligent. As requested by the parties, and for the reasons set forth in the concurrently filed memorandum disposition, we vacate Alba's conviction and sentence for conspiracy to manufacture and distribute Ecstasy. We also hold that the techniques the government used to monitor Alba's e-mail and Internet activity did not constitute a search for Fourth Amendment purposes and that, whether or not the monitoring came within the scope of the then-applicable pen register statute, Alba is not entitled to the suppression of evidence obtained through the monitoring. Accordingly, we affirm Alba's other convictions and sentences, meaning that his prison term remains 360 months while his supervised release term is reduced from six to five years.

Forrester's conviction and sentence are **REVERSED**. Alba's convictions and sentences are **AFFIRMED IN PART AND REVERSED IN PART**.