Mail Cover Surveillance: Problems and Recommendations

Steven R. Morrison
Reporter, NACDL
Vice-Chair, Fourth Amendment Advocacy Committee

April 19, 2015

Introduction

Mail cover surveillance ("mail covers"), which is the investigative practice of recording the information listed on the outside of mail going to or from a designated address, has existed since the nineteenth century.[1] While often a legitimate tool of criminal investigations, mail covers have been abused. They were used in the 1950s against suspected communists and expanded to include surveillance of the contents of letters.[2] Indeed, CIA and FBI agents used mail covers to intercept hundreds of thousands of letters in the 1950s and 1960s, sometimes smuggling them out of post offices to open and read them to avoid postal worker intervention.[3]

It was only after a fifteen year-old girl was targeted in the 1970s for sending a letter to the Socialist Workers Party as a class assignment that the abuses came to light.[4] As a result of these abuses, mail cover regulations were promulgated in 1975, and now appear at 39 C.F.R. § 233.3.[5] Based on concerns about the vagueness and overbreadth of

---

[1] David S. Kris & J. Douglas Wilson, *In General*, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 21:1.
[2] *Id.*
[3] *Id.*
[4] *Paton v. La Prade*, 469 F.Supp. 773 (D.N.J. 1978); *Mail Snooping Needs More Accountability*, DES MOINES REGISTER, Oct. 30, 2014.
[5] Kris & Wilson, *supra* note 1.

authorizing mail covers for "national security," the regulations were amended in 1979 to include a more precise definition of that term.[6]

Despite these reforms, concerns about mail covers have persisted. In 1986, the *South Florida Sun-Sentinel* expressed concern that mail covers doubled from 1978 through 1985, from 4,379 to 8,597.[7] The September 11, 2001 terrorist attacks prompted the Bush Administration to seek expanded mail cover authority, a move that concerned both the Postal Service and privacy and civil rights advocates.[8] In the eleven years since 2001, local, state, and federal law enforcement agencies made more than 100,000 requests for mail covers.[9] One of these requests came from Maricopa County Sheriff Joe Arpaio to monitor the mail of Mary Rose Wilcox, a frequent critic of Arpaio and a Maricopa County supervisor.[10] Wilcox sued the county and won a $1 million settlement.[11] In the early 2000s, federal prosecutors used a mail cover to monitor the communications between a criminal defendant and his lawyers.[12] In 2013, a former member of the Earth Liberation Front and a current bookstore owner learned his mail was being tracked.[13] In response, a former Justice Department official said the current regime does not track criminal suspects, but the approach seems to be, "Let's record everyone's mail so in the future we might go back and see who you were communicating with."[14]

[6] *Id.*
[7] *Government Surveillance of Suspect Mail is Doubled*, SOUTH FLORIDA SUN-SENTINEL, Mar. 2, 1986.
[8] Eric Lichtblau, *Bush Plan Would Let FBI Track Mail*, DESERET MORNING NEWS, May 21, 2005.
[9] Ron Nixon, *Report Reveals Wider Tracking of Mail in U.S.*, NEW YORK TIMES, Oct. 27, 2014.
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Ron Nixon, *U.S. Postal Service Logging All Mail for Law Enforcement*, NEW YORK TIMES, July 3, 2013.
[14] *Id.*

Most recently, the *Washington Post* reported that the U.S. Postal Service almost never denies applications for mail covers.[15]

A 2014 U.S. Postal Service audit of the mail cover program revealed the breadth of the mail cover program as well as its systemic failures in authorization and monitoring.[16] In 2013 alone, the Postal Service processed about 49,000 mail covers.[17] The report detailed the following violations of the governing regulation:

- 21 percent of requests were approved without written authority;
- 13 percent of requests were not adequately justified or reasonable grounds for them were not transcribed accurately;
- 27 percent of requests were not entered into the application in a timely fashion;
- 61 percent of accountable documents were not returned on time;
- 32 percent of case files did not include the dates that Postal Inspectors visited facilities where mail covers were processed;
- 10 percent of case files did not have the dates of the mail period coverage or mail counts;
- 15 percent of inspectors did not have the required nondisclosure form on file;
- 32 percent of case files were not returned to the Postal Inspection Service Office of Counsel in a timely fashion after the mail cover period ended;
- Mail cover requests were not always processed in a timely fashion;

[15] Josh Hicks, *Postal Service Almost Never Denies Mail-Surveillance Requests*, WASHINGTON POST, Dec. 30, 2014.
[16] Office of the Inspector General, United States Postal Service, *Postal Inspection Service Mail Covers Program*, May 28, 2014.
[17] *Id*. at 1.

- Officials did not periodically review the criminal programs as required.[18]

The audit reported that inadequate controls generated these failures.[19] Officials at seven postal facilities cited their focus on mail processing and employee turnover as primary reasons for inadequate controls.[20] The audit finally recommended improved controls for mail cover processing, timeliness, and data integrity, and establishing procedures for periodic reviews of mail covers.[21]

It remains unknown whether these or other recommendations will be taken up. In the meantime, constitutional and privacy concerns persist. This report addresses these concerns. To do so, it is organized as follows. In Part I, the report describes mail covers and 39 C.F.R. § 233.3, which is the sole authority governing mail covers. In Part II, the report sets forth the relevant law. This law primarily is that of the Fourth Amendment, especially involving the potential impact of *United States v. Jones*,[22] the 2012 GPS tracking case. It also includes, to a lesser degree, First Amendment law on association, receipt of information, and anonymity. Part III discusses three potential constitutional and privacy issues generated by mail cover surveillance. These issues are (1) whether mail covers ever entail a Fourth Amendment violation; (2) whether § 233.3, if it is followed, is adequate to protect Fourth Amendment rights; and (3) whether § 233.3 is adequate to protect sub-Fourth Amendment privacy concerns (this issue assumes that there *are* such sub-constitutional privacy issues, and this portion of the report discusses them). Finally, Part IV proposes a set of recommendations that should protect

[18] *Id*. at 2-6.
[19] *Id*. at 3-4.
[20] *Id*. at 4.
[21] *Id*. at 6-7.
[22] 132 S.Ct. 945 (2012).

individuals' privacy, improve systemic mail cover controls, and ensure that legitimate law enforcement efforts are not hindered.

I. Mail covers and 39 C.F.R. § 233.3

39 C.F.R. § 233.3 provides "the sole authority and procedure for initiating a mail cover, and for processing, using and disclosing information obtained from mail covers."[23] Section 233.3 defines a mail cover as

> the process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter, or by which a record is made of the contents of any unsealed class of mail matter as allowed by law, to obtain information in order to: (i) Protect national security, (ii) Locate a fugitive, (iii) Obtain evidence of commission or attempted commission of a crime, (iv) Obtain evidence of a violation or attempted violation of a postal statute, or (v) Assist in the identification of property, proceeds or assets forfeitable under law.[24]

The USPS is supposed to maintain "rigid control and supervision" over mail covers.[25] The Chief Postal Inspector is the principal officer supervising mail covers. He may delegate any or all authority to a limited number of designees,[26] who may authorize mail covers in response to a written request, stating a reason to believe the mail cover will produce evidence of a violation of a postal statute or reasonable grounds to demonstrate the mail cover is necessary to protect national security, locate a fugitive, obtain information regarding a crime, or assist in the identification of forfeitable assets.[27] When time is of the essence, an oral request for a mail cover may be acted upon.[28]

[23] 39 C.F.R. § 233.3(b).
[24] § 233.3(c)(1).
[25] § 233.3(a).
[26] § 233.3(d).
[27] § 233.3(e).
[28] § 233.3(e)(3).

With some exceptions, not vital to this report, postal officials may not record mail cover information in the absence of a mail cover order.[29] In addition, they may not open, inspect the contents of, or permit such inspection of sealed mail without a federal search warrant.[30] Mail cover orders are not to include correspondence between a target and her known attorney.[31]

Except to locate a fugitive or for national security investigations, mail cover orders remain in effect for only thirty days. They may be extended with adequate justification, and new thirty-day periods may be authorized.[32] Mail cover orders may last longer than 120 days only with the personal approval of the Chief Postal Inspector or his designees at National Headquarters.[33] Except to locate fugitives, mail cover orders are ineffective once a target has been indicted or an information has issued. If a target is being investigated for further crimes or to locate her assets for forfeiture, a new mail cover order may issue.[34] National security mail cover requests must be approved personally by the head of the law enforcement agency requesting the cover or a designee at the agency's headquarters level. This request must be transmitted, in writing, to the Chief Postal Inspector.[35]

The Chief Postal Inspector is to have custody of all mail cover requests, records of actions ordered thereon, and all reports generated pursuant thereto.[36] If the Chief Postal Inspector or his designee determines that a mail cover was improperly ordered, all

[29] § 233.3(f)(1) (These exceptions include undelivered mail found abandoned or in the possession of a person reasonably believed to have stolen or embezzled such mail; damaged or rifled, undelivered mail; or mail posing an immediate threat to persons or property.).
[30] § 233.3(g)(1).
[31] § 233.3(g)(3).
[32] § 233.3(g)(5).
[33] § 233.3(g)(6).
[34] § 233.3(g)(7).
[35] § 233.3(g)(8).
[36] § 233.3(h)(1).

data acquired as a result of the order is to be destroyed and the requesting authority notified of the discontinuance of the mail cover.[37] Data generated from a mail cover is to be available to a target through appropriate discovery procedures,[38] and the data is to be retained for eight years.[39]

The Chief Postal Inspector or his designee at Inspection Service Headquarters is to periodically review mail cover orders issued to ensure compliance with § 233.3.[40] A separate periodic review of national security mail cover orders is mandated.[41] The Chief Postal Inspector's determination in all matters involving mail covers is final and conclusive, and is not subject to further administrative review.[42]

Section 233.3 does not apply to the military postal system.[43]

II. Relevant law: Fourth and First Amendments

Mail covers are potentially limited by the Fourth Amendment as well as First Amendment rights to associate, to receive information, and to anonymity.

a. Fourth Amendment: *Ex Parte Jackson*

In 1877, the United States Supreme Court in *Ex Parte Jackson* held that the Fourth Amendment protects the contents of letters and sealed packages subject to letter postage from inspection in the absence of a warrant or other justification.[44] The Court also ruled, however, that the Fourth Amendment did not protect letters' and packages' "outward form and weight."[45] As to "printed matter" (advertisements, bulk mail, and

[37] § 233.3(h)(2).
[38] § 233.3(h)(3).
[39] § 233.3(h)(4).
[40] § 233.3(j)(1).
[41] § 233.3(j)(2).
[42] § 233.3(j)(3).
[43] § 233.3(k).
[44] *Ex Parte Jackson*, 96 U.S. 727, 733 (1877).
[45] *Id*.

other mail open to examination), the Court held that contents may be inspected but transportation of such matter could not be regulated "so as to interfere in any manner with the freedom of the press."[46]

Jackson, therefore, stood for three propositions. First, the Fourth Amendment protects the contents of letters and packages that senders generally consider private. Second, the Fourth Amendment does *not* protect information on mail covers. Third, mail has both Fourth Amendment and First Amendment implications.

b. Fourth Amendment: *Katz v. United States*

The U.S. Supreme Court's opinion in *Katz v. United States* set forth the familiar two-part privacy test for implicating the Fourth Amendment.[47] Under the *Katz* test, an individual is protected by the Fourth Amendment in areas where she has an actual (subjective) expectation of privacy, and when that expectation is one that society is prepared to accept as reasonable.[48] *Katz*, moreover, generally reaffirmed *Ex Parte Jackson*.[49]

As *Katz* tracked the holding in *Jackson*, which protected the contents of mail but not the information on mail covers, courts have uniformly held that mail covers usually do not violate the Fourth Amendment.[50] At least one court, however, has left open the possibility that mail covers that extend beyond their proper scope may generate Fourth Amendment violations.[51] To date, however, violations of § 233.3 have not resulted in suppression of evidence. The justification for the lack of suppression is that although

[46] *Id*.
[47] 389 U.S. 347 (1967).
[48] *Id*. at 361 (Harlan, J., concurring).
[49] *Id*. at 351-52.
[50] Daniel E. Feld, *Validity, Under Fourth Amendment, of "Mail Cover"*, 57 A.L.R. FED. 742 (1982).
[51] *United States v. Huie*, 593 F.2d 14, 15 (5th Cir. 1979).

violations of mail cover regulations lead to unauthorized surveillance, the information surveilled is not protected by *Katz* and the Fourth Amendment. The violation is therefore merely regulatory, not constitutional, and thus suppression is unavailable.[52]

c. Fourth Amendment: *United States v. Jones*

In 2012, the Supreme Court issued its opinion in *United States v. Jones*,[53] which is a potential basis for successful Fourth Amendment challenges to mail covers where *Katz*-based challenges have been unsuccessful. In that case, the Court held that the attachment of a GPS device to a suspect's car, which was then used to track the suspect on public streets for twenty-eight days, was a Fourth Amendment search.[54] Justice Scalia, writing for the majority, based the opinion on the trespass model of the Fourth Amendment, in which government agents perform Fourth Amendment searches when they physically enter or access private property to obtain information.[55]

While Justice Scalia discounted the validity of the *Katz* privacy test in favor of the trespass approach,[56] Justices Sotomayor and Alito, concurring, ensured that *Katz* remains good law.[57] Alito went a step further, basing his opinion in part on what some scholars have called the "mosaic theory" of the Fourth Amendment, pursuant to which a Fourth Amendment search occurs when government agents observe enough publicly

[52] *United States v. Hinton*, 222 F.3d 664, 674 (9th Cir. 2000); *United States v. Felipe*, 148 F.3d 101, 109 (2d Cir. 1998) (*citing U.S. v. Caceres*, 440 U.S. 741, 755-57 (1979)); *United States v. Loudon*, 2009 WL 88339, *1-2 (D.Vt.); Kris & Wilson, *supra* note 1.
[53] 132 S.Ct. 945 (2012).
[54] *Id*. at 949.
[55] *Id*.
[56] *Id*. at 953.
[57] *Id*. at 954-55, 959-60 (Sotomayor, J., concurring; Alito, J., concurring).

ascertainable conduct or information to create a picture of a suspect so detailed as to meet the *Katz* privacy test.[58] He wrote,

> [R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable . . . But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving . . . I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.[59]

Jones presents two possible arguments against the constitutionality of some mail covers. First, Justice Scalia's trespass argument may lead courts to conclude that mail covers entail "occupying" an individual's private property, namely the envelope that she sends through the mail, and are therefore searches. Second, Justice Alito's mosaic theory argument may lead courts to conclude that mail covers of long duration comprise searches. Both approaches would result in some mail covers being deemed Fourth Amendment searches. They would, therefore, have to be initiated by a search warrant or other justification; satisfaction of § 233.3's requirements would not be sufficient to overcome the constitutional hurdle.

The trespass argument has some merit in the mail cover context. Just as someone who drives her car on a public street relinquishes her right to hide the appearance of her car and her location at any given moment, but does not relinquish her possessory interest in the car, someone who sends a letter in the mail relinquishes and retains the same interests. However, Justice Scalia's trespass argument depended upon government agents

[58] *United States v. Katzin*, 732 F.3d 187, 237 n. 23 (3d Cir. 2013); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).
[59] *Jones*, 132 S.Ct. at 964.

"occupying" private property by placing a device on someone's car. In contrast, mail covers simply gather information from the outside of an envelope or package; they do not attach anything to private property. That said, the trespass involved in mail covers is that government officials must take possession of and detain, if only for a brief moment, private property in a way that they would not possess and detain it if they were merely processing mail for delivery. While attaching a GPS device to a car is more obviously a trespass than handling mail for a mail cover, the difference can be viewed as one of degree, and not quality. As such, the *Jones* trespass theory may provide a basis for Fourth Amendment mail cover challenges.

The mosaic theory argument is more convincing in one way, and less convincing in another way, than the trespass argument. It is more convincing because the very purpose of a mail cover is to establish a target's network of people with whom she communicates. This type of information is not available unless the target is surveilled persistently and over a period of days. Mail covers are virtually explicitly meant to create a mosaic. Furthermore, the maximum initial regulatory period of mail covers is thirty days — two days longer than the twenty-eight day period considered in *Jones* (one suspects that virtually all mail covers are authorized for at least thirty days, no less). *Jones*, therefore, speaks directly to the mail cover regime. However, the basis for this argument is not the originalist, well-established trespass approach, but the novel, academic mosaic theory. For a court to hold that mail covers are Fourth Amendment searches, it would have not only to find so under either *Katz* or *Jones*, but also to adopt the mosaic theory. The time may not yet be ripe for such a jurisprudential innovation.[60]

[60] *See, e.g., United States v. Cuevas-Perez*, 640 F.3d 272, 284 (7th Cir. 2011); *In re Application of F.B.I.*, 2014 WL 5463097, *10 (FISC); *United States v. Graham*, 846 F.Supp.2d 384, 390-91 (D.Md. 2012).

d. First Amendment: *Paton v. La Prade*

While most courts have rejected First Amendment arguments against mail covers on the grounds that surveillance of the outside of mailings cannot infringe upon free speech,[61] others have claimed that the First Amendment is implicated because mail cover data reveals much about a target's "relationships with both individuals and organizations."[62]

In *United States v. Gering*, the Ninth Circuit rejected a defendant's argument that mail covers entail *per se* violations of the First Amendment, but suggested that there may be a violation in cases where a defendant can demonstrate an actual First Amendment burden.[63] In another case, the Ninth Circuit implied that mail covers might violate the First Amendment when initiated for the purpose of abridging First Amendment freedoms.[64]

The major case presenting a First Amendment challenge to mail covers was *Paton v. La Prade*.[65] In that case, Lori Paton was enrolled in her high school's social studies course. To complete one of her assignments, Paton wrote a letter to the Socialist Labor Party requesting information about its program, policies, and positions.[66] Paton inadvertently addressed the letter to The Socialist Workers Party, against which the FBI had initiated a mail cover.[67]

---

[61] *United States v. Choate*, 576 F.2d 165, 180-81 (9th Cir. 1978); *Cohen v. United States*, 378 F.2d 751, 760 (9th Cir. 1967). Indeed, the recent decision *ACLU v. Clapper*, which upheld the government's bulk telephony metadata collection program, looked for support to prior courts' rejection of First Amendment arguments against mail covers. 959 F.Supp.2d 724, 753 (S.D.N.Y. 2013).
[62] *Choate*, 576 F.2d at 203 (Hufstedler, J., concurring and dissenting).
[63] 716 F.2d 615, 620 (9th Cir. 1983); *see also United States v. Mayer*, 490 F.3d 1129, 1137 (9th Cir. 2007).
[64] *United States v. Aguilar*, 883 F.2d 662, 705 (9th Cir. 1989).
[65] 469 F.Supp. 773 (D.N.J. 1978).
[66] *Id*. at 774-75.
[67] *Id*. at 775.

When the FBI obtained Paton's letter, it opened an investigation on her for "subversive" matter, and a field investigation ensued. It soon became local and national news that Paton was the subject of an FBI investigation.[68]

The district court found that Paton had the First Amendment right to receive her requested information "free of government interference and to remain anonymous in her request for political information."[69] The court also, however, limited its holding to national security cases, finding that they "often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime."[70] The court therefore addressed only mail covers involving national security, ultimately holding that "[n]ational security as a basis for the mail cover is unconstitutionally vague and overbroad."[71]

In a more recent case, a former member of the Earth Liberation Front and a current bookstore owner, Leslie Pickering, learned his mail was being tracked.[72] In that case, the post office accidently sent to Pickering a card ordering the mail cover and reading, "Show all mail to supv" — supervisor — "for copying prior to going out on the street." It included Pickering's name, address and the type of mail that needed to be monitored. The word "confidential" was highlighted in green. The post office confirmed to Pickering that it was tracking his mail, but would say nothing else.

These cases suggest three potential First Amendment challenges to mail covers. While not strictly prohibiting communication or directly infringing upon First

[68] *Id*. at 776.
[69] *Id*. at 778.
[70] *Id*. at 781.
[71] *Id*. at 782.
[72] Nixon, *supra* note 13.

Amendment rights, mail covers may chill individuals' right to associate,[73] to receive information,[74] and to engage in First Amendment activity anonymously.[75] To be sure, Paton and Pickering knew they were being monitored — often a requirement for a successful First Amendment claim because it is thought that without knowledge of monitoring, the monitoring cannot chill First Amendment activities.[76] Without knowledge, there can often be no standing.[77] However, the standing requirement has been relaxed for First Amendment overbreadth claims, allowing litigants to challenge a law "not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute's very existence may cause others not before the court to refrain from constitutionally protected speech or expression."[78]

III. Three issues

Based on the mail cover regime and the relevant law, there are three potential constitutional and privacy issues generated by mail cover surveillance. These issues are (1) whether mail covers ever entail a Fourth Amendment violation; (2) whether § 233.3, if it is followed, is adequate to protect Fourth Amendment rights; and (3) whether § 233.3 is adequate to protect sub-Fourth Amendment privacy concerns.

a. Do mail covers ever entail a Fourth Amendment violation?

Courts have uniformly held that mail covers do not entail Fourth Amendment violations because they function to reveal only information that is already readily visible to anyone who observes the mailing. Under the *Katz* expectation of privacy test, courts

[73] *N.A.A.C.P. v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958).
[74] *Kleindienst v. Mandel*, 408 U.S. 753, 762 (1972).
[75] *McIntyre v. Ohio Elections Com'n*, 514 U.S. 334, 342 (1995).
[76] *Cooksey v. Futrell*, 721 F.3d 226, 236 (4th Cir. 2013); *Toscano v. Lewis*, 2013 WL 1632691, *5 (N.D.Cal.).
[77] *See Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138 (2013).
[78] *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973).

have held that no one has a reasonable expectation of privacy in the information contained on mailings' external packaging.

Since *Jones*, however, no court has considered the constitutionality of mail covers under the Fourth Amendment. *Jones* presents a potential for mail covers to be found unconstitutional in some cases where the mail cover surveillance was particularly long-lasting and invasive. There are three notable issues in this analysis.

First, the length of time the mail cover is in place matters for two reasons. A period of twenty-eight days of GPS tracking in *Jones* was too long to satisfy the Fourth Amendment, though the Court refrained from setting a constitutionally permissible period of time during which agents could track a suspect via GPS without a warrant. The first reason that the length of time matters in the mail cover context is simply that it mattered in *Jones*. The second reason that it matters is that § 233.3 authorizes mail covers for renewable thirty-day periods. Each period is therefore two days longer than *Jones*' twenty-eight days. The length of time a mail cover is in effect could, therefore, implicate the Fourth Amendment in two ways: the length of time could entail a violation, and § 233.3 itself, authorizing a thirty-day period, could itself be held unconstitutional, at least as applied in certain cases.

Second, the intensity of the search matters. Justice Alito's opinion in *Jones* rested in part on how much information officers could glean from a persistent GPS tracking of the defendants. In turn, how intensive a mail cover is could contribute to whether it violates the Fourth Amendment.

Third, whether proper procedures were followed matters. Justice Scalia's opinion in *Jones* rested on a trespass theory, which could have been overcome had the officers in

that case executed their search warrant in a timely fashion. Just as proper police procedures in *Jones* could have led to an avoidance of the trespass-based Fourth Amendment violation, so could following § 233.3 in the mail cover context. At the very least, whether the mail cover regulations were followed could *contribute* to a finding of constitutionality or unconstitutionality.

The important upshot is that if a mail cover is found to have entailed a Fourth Amendment violation, then suppression of resulting evidence is an option. However, if only § 233.3 was violated, then suppression is not available.

b. Is § 233.3 adequate to protect Fourth Amendment rights?

Most provisions of § 233.3 are untroubling from a strictly Fourth Amendment point of view. Sections (g)(5) and (g)(6), however, present potential constitutional problems. Section (g)(5) provides for a thirty-day period of mail monitoring, with thirty-day extensions only with "adequate justification." Section (g)(6) provides for a maximum 120-day continuous period of monitoring, with extensions beyond that only if personally approved by the Chief Postal Inspector or his designees at National Headquarters.

There are two ways that these provisions could violate the Fourth Amendment. First, as noted above, *Jones* could be interpreted to mean that even an initial thirty-day period of monitoring is unconstitutional without a search warrant. Second, *Jones* should likely be interpreted to mean that a mail cover *at some point of duration* becomes unconstitutional in the absence of a search warrant. How long that period is could depend upon at least two factors.

First, it could depend upon how courts understand the value and volume of information gleaned from a mail cover. If the value and volume is viewed as similar to that of GPS tracking, as in *Jones*, then the acceptable time period should roughly track that of future cases that refine *Jones*. Twenty-eight days of monitoring could, in light of *Jones*, constitute a violation.

Second, it could depend upon the safeguards in place. In *Jones*, the government agents had an expired search warrant, which the Court effectively treated as no search warrant at all. Therefore, in *Jones*, safeguards were entirely lacking. Section 233.3 does, however, provide some safeguards. If followed, they could serve to make mail covers more "reasonable" for Fourth Amendment purposes and thus enlarge the period of time mail covers are constitutionally permissible. Conversely, if § 233.3 is not followed, such a regulatory violation might decrease the amount of time a mail cover may be constitutionally in effect.[79]

c. Is § 233.3 adequate to protect sub-Fourth Amendment privacy issues?

Whether § 233.3 is adequate to protect sub-constitutional privacy issues — i.e. privacy interests that are not protected by the Fourth Amendment — depends upon a normative assessment of what those issues are. Section 233.3 raises a number of them, involving who authorizes of mail covers; evidentiary standards and procedures for authorization; reliability of evidence supporting authorization; and retention of evidence gleaned from mail covers. A final issue, that of the duration of mail covers, is detailed above and not repeated here.

[79] To be sure, courts prior to *Jones* did not consider a regulatory violation in their Fourth Amendment analyses. This was so because the information gleaned was in plain view, so there could be no Fourth Amendment violation. Post-*Jones*, however, lengthy surveillance of people and information in plain view at some point violates the Fourth Amendment. The question is when. The duration of time matters, but so too should the presence of safeguards and whether procedures were followed.

The first potential privacy issue concerns the people who may authorize mail covers. Section 233.3(d) provides that the Chief Postal Inspector or his designees may authorize mail covers, and § 233.3(j)(3) makes these authorizations "final and conclusive and not subject to further administrative review." This is problematic for three related reasons. First, mail covers are being authorized by postal inspectors, and not judges, who have experience evaluating evidence, applying evidence to evidentiary standards, and judging credibility of witnesses and affiants. Second, the evidence presented by law enforcement agents to postal inspectors is not presented under oath in an affidavit, nor is its presentation subject to the penalties of perjury. Third, there appears to be little scrutiny of the reliability of evidence presented to postal inspectors.

The second potential privacy issue is that there appears to be no appellate process in place to correct for errors, negligence, or willful misrepresentation. In short, the process of authorization appears siloed, impervious to external criticism, and not based on any critical analysis of evidence provided in mail cover applications.

The evidentiary standards and procedures for authorization exacerbate the problems inherent in the process of authorization. While mail cover applications must be made in writing,[80] they need only state a "reasonable grounds to demonstrate the mail cover is necessary to" further the legitimate purposes of a mail cover (to protect the national security, locate a fugitive, etc.).[81] The "reasonable grounds" standard is generally applied to brief, superficial law enforcement encounters with individuals, like *Terry* stops and brief, on-the-street seizures.[82] These stops and seizures are meant to permit law enforcement agents to quickly determine whether crime is afoot in as short a

[80] 39 C.F.R. § 233.3(d)(3).
[81] 39 C.F.R. § 233.3(e)(2).
[82] *Illinois v. Wardlow*, 528 U.S. 119 (2000); *Terry v. Ohio*, 392 U.S. 1 (1968).

time as possible. They are not meant to justify persistent, invasive surveillance like a mail cover. The "reasonable grounds" standard that justifies mail cover orders seems excessively deferential to law enforcement in relation to the resulting surveillance and in comparison to other government actions justified by the same standard.

To make matters worse, there appears to be no requirement that agencies that request a mail cover must meet any level of evidentiary reliability. The rules of evidence do not apply, nor are they even admonitory guidelines; applicants need not file affidavits under oath; no hearings are held, as they are for search warrant applications; it seems sufficient merely to state — with no evidence whatsoever — that a mail cover is necessary; and there is no provision for a *Franks* hearing or its equivalent to test the truthfulness of the contents of an application. Because suppression is not available in the mail cover context, there is no deterrent to either negligent or intentionally bad police conduct or rubber-stamping of applications.

Once a mail cover is in place, postal agents begin to collect data on a target's sent and received mail. This data must be stored for eight years.[83] This is quite a long period of time, exceeding by three years even the storage period of data the National Security Agency generates in its bulk telephony metadata program, which Edward Snowden revealed.[84] If privacy advocates have been concerned with the lengthy storage of mounds of telephony metadata[85] and, as another example, automatically collected data on date-

[83] 39 C.F.R. § 233.3(h)(4).
[84] *Klayman v. Obama*, 957 F.Supp.2d 1, 37 (D.D.C. 2013).
[85] In response, President Obama last year advanced a policy to end the bulk storage of such metadata. *Obama to end NSA's mass storage of telephone metadata*, REUTERS, Jan. 17, 2014, available at http://www.cnbc.com/id/101345381#.

stamped locations of automobiles,[86] they should also be concerned with this eight-year storage of mail cover data.

IV. Remedies and recommendations

There are a number of potential and actual problems with the current mail cover regime. First, there appear to be systemic failures to follow § 233.3 with regard to authorization, justification, processing, oversight, and recordkeeping. Second, *United States v. Jones* opens the possibility that at least some mail covers may violate the Fourth Amendment. Third, even if § 233.3 is followed such that there is no Fourth Amendment violation, mail covers may violate some sub-constitutional principles of privacy because there are siloed and unreviewable authorization procedures, low evidentiary standards for authorization, no checks on the reliability of such evidence, an eight-year data retention mandate, and potential problems with the duration of mail covers. This section outlines remedies and recommendations, including litigation strategies, to address these problems.

a. Systemic failures to follow § 233.3

At a minimum, government agents ought to follow their own regulations. NACDL therefore seconds the OIG's recommendation to improve managerial controls over authorization, processing, oversight, and reviews of mail cover program protocols. These improved controls, however, are only as good as the enforcement mechanisms that ensure them. Congress should, therefore, considering passing a law that requires suppression of evidence gleaned from a mail cover if the evidence was obtained during the course of a reckless or intentional violation of § 233.3. This standard would not penalize agents who occasionally do not follow § 233.3 provisions because of their focus

[86] Bennett Stein, *FOIA Documents Reveal Massive DEA Program to Record American's Whereabouts With License Plate Readers*, ACLU, Jan. 26, 2015, available at https://www.aclu.org/blog/technology-and-liberty-criminal-law-reform/foia-documents-reveal-massive-dea-program-record-ame.

on, say, mail processing or employee turnover,[87] but would require them to ensure that, over time, these resource issues are not used as an excuse to maintain an illegal mail cover program.[88]

b. The *United States v. Jones* remedy

Katz has never been an effective basis for arguing that mail covers violate the Fourth Amendment because the expectation of privacy in the outside of a mailing is not reasonable. *United States v. Jones*, however, has opened new avenues for Fourth Amendment arguments against mail covers. Defense attorneys should use *Jones* to argue for Fourth Amendment violations and therefore for suppression of evidence generated by mail covers. They can do so in four ways.

First, as a general matter, attorneys should use *Jones* to argue that the plain view doctrine is infirm in the age of mass, persistent surveillance. Because government agents are able to persistently and easily monitor suspects over time, they can generate a mosaic image of a suspect with information available only in plain view. As in *Jones*, this means that the *Katz* expectation of privacy test may have new vitality, even where agents surveille suspects or data solely in plain view.

Second, and specifically regarding certain mail covers, attorneys should argue that some mail covers entail surveillance for an excessive and therefore unconstitutional length of time. *Jones*' twenty-eight-day period offers a grounded baseline.

[87] Lack of resources has, indeed, been claimed by postal authorities as a reason for failure to comply with § 233.3. Office of the Inspector General, United States Postal Service, *Postal Inspection Service Mail Covers Program*, May 28, 2014.

[88] This approach can be compared to Fourth Amendment law on maintaining warrant databases, pursuant to which negligent maintenance of databases does not warrant suppression, but that systemic, reckless, or intentional failure to maintain databases may result in suppression. *See Herring v. United States*, 129 S.Ct. 695 (2009).

Third, attorneys can argue that mailings consist of senders' private property, such that any government action upon such mailing (beyond that which is necessary to process the mailing) is a trespass. In the absence of a warrant (which § 233.3 does not, of course, require), any information gleaned from such trespass must be suppressed under *Jones*.

Fourth, attorneys can argue that failure to follow the provisions of § 233.3 contribute to the unreasonableness and thus unconstitutionality of any subsequent search. To be sure, prior courts have rejected such arguments, concluding that a violation of a regulation, in the absence of a Fourth Amendment violation, does not make suppression available. However, *Jones* may convince courts that a mail cover can be a Fourth Amendment search. If it does, then the question of the reasonableness of that search arises. Any regulatory violation could contribute to a finding of unreasonableness.

c. Siloed and unreviewable authorization procedures

Currently, the decisions of the Chief Postal Inspector or his designees regarding mail covers are unreviewable. This violates basis principles of due process and checks and balances, and has resulted in abuses throughout the history of the mail cover program. NACDL recommends the creation of a review or appellate-type system. This system cannot be based upon suspects or their attorneys challenging mail covers, since to be effective mail covers must be secret. The system should, therefore, be housed in the government. Much like current proposals to have a privacy advocate in Foreign Intelligence Surveillance Courts to challenge what have been viewed as one-sided, rubber-stamping procedures to obtain surveillance orders in the national security context,[89] mail cover procedures should be subject to similar internal controls.

[89] Denver Nicks, *Privacy Advocates Call for FISA Court Reform*, TIME, July 10, 2014, available at http://time.com/2970766/privacy-freedom-act-reform-secret-nsa-oversight-fisa/.

d. Low evidentiary standard and unreliable evidence

Currently, mail cover authorizations require only reasonable grounds, and there exist no apparent checks on the reliability of evidence presented to support such a low evidentiary standard. This low bar has been criticized in the national security context, and should be addressed in the mail cover context. Section 233.3(e)(2) provides that one may authorize a mail cover "when the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary." NACDL recommends that this provision be altered to authorize a mail cover "when the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary *and the Chief Postal Inspector or his designee concludes there are articulable facts, based on reliable evidence, to believe the mail cover is necessary*."

The authorizing person should then be required to record and maintain the articulable facts and reasons the supporting evidence is reliable. During a subsequent criminal proceeding, suppression of evidence should be an available remedy if a judge determines that there were no articulable facts or the evidence supporting them was unreliable.

e. Eight-year data retention mandate

There appears to be no justification for maintaining mail cover data for eight years; if national security-related telephony metadata is retained only for five years, the retention of more mundane mail cover data for eight years seems arbitrary. NACDL recommends that the Postal Service and Congress consider revising that period down. While a certain period of data retention is justified — both for law enforcement purposes and to protect potential defendants' rights — that period should be grounded in reason.

Conclusion

While mail covers have been used since the nineteenth century, their benefit to law enforcement must be analyzed in light of their demonstrated abuses. The 2014 OIG report is just the latest evidence that the mail cover program is not always followed according to law. Even if the law were followed, Fourth Amendment and privacy concerns persist.

This report has detailed the mail cover program, its abuses and systemic failures, the relevant law, and has provided a set of recommendations that can protect individuals' privacy while permitting law enforcement agents to use mail covers to effectively investigate crime. In the post-*Jones* and national security era, addressing the potential for mail covers to violate the Fourth Amendment and privacy norms is more important than ever.

* * *