NOTES

Going Postal: Analyzing the Abuse of Mail Covers Under the Fourth Amendment

Since at least the late 1800s, the United States government has regularly tracked the mail of many of its citizens. In 2014 alone, for example, the government recorded all data on the outside of the mail parcels of over 50,000 individuals via a surveillance initiative known as the mail covers program. In the current age of mass surveillance, this program—like all surveillance initiatives—has grown exponentially. Unbeknownst to most citizens, the government now photographs and records the exterior of each of the roughly 160 billion mail parcels delivered by the USPS every year. Still, despite its ability to allow governmental authorities to uncover a startlingly accurate picture of citizens' daily lives, the long-abused mail covers program continues to be implemented without any judicial oversight. This Note provides the first comprehensive legal analysis of the mail covers program in the modern era. In doing so, it also analyzes current Fourth Amendment jurisprudence and advocates for the adoption of the mosaic theory to privacy protection better capable of safeguarding citizens in an age of unprecedented government surveillance capability.

When you control the mail, you control information.[1]
—Newman

INTRODUCTION

President Jimmy Carter once famously stated that he uses snail mail rather than electronic communications when he wishes to speak to foreign leaders in his retirement.[2] Like many Americans in the wake of Edward Snowden's alarming data privacy revelations in 2013, President Carter fears that his emails may be monitored by government authorities, and strives to use traditional mail services to evade Big Brother's prying eyes.[3] Unfortunately for President Carter and other privacy-conscious Americans, however, traditional mail services have themselves been an integral part of government surveillance initiatives for centuries.

Using a surveillance technique known as a "mail cover," the United States government has regularly tracked the mail of many of its citizens since at least the mid-nineteenth century, recording all information on the outside of their mail parcels.[4] In 2014 alone, for example, the United States Postal Service ("USPS" or "Postal Service") processed a startling 57,000 mail covers.[5] This means that throughout 2014 the USPS documented, at the request of law enforcement agencies, the addresses, return addresses, postal dates, and other information appearing on the outside of each parcel of mail sent and

1. *Seinfeld: The Lip Reader* (NBC television broadcast Oct. 28, 1993).

2. David Jackson, *Carter Uses Snail Mail to Evade NSA*, USA TODAY (Mar. 24, 2014), http://www.usatoday.com/story/theoval/2014/03/24/obama-jimmy-carter-national-security-agency-surveillance-snail-mail/6818605/ [https://perma.cc/7B44-NBUJ].

3. *Id.*

4. *See, e.g.*, DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 21.1 (2d ed. 2012).

5. *See infra* note 46.

received by over 50,000 individuals for extended periods of time.[6] In addition, recent technological innovations have allowed the USPS to begin photographing and recording the outside of each of the roughly 160 billion mail parcels it handles each year.[7] Remarkably, all of this surveillance occurs without any judicial oversight.

Due to the highly secretive nature of mail covers, it also occurs largely without opportunity for postsurveillance corrective litigation. The Supreme Court has never addressed the mail covers program, and the program has been only sparingly litigated in lower courts. In the few cases in which the program has been challenged, [8] it has been held constitutional, in large part because of the apparent alignment of mail covers with the third-party doctrine, one of the basic tenets of modern Fourth Amendment jurisprudence.[9] This doctrine holds that an individual accepts the risk that her otherwise private personal information may be turned over to government authorities when she willingly reveals that information to a third party, be it another person, a telephone company, or, as here, the Postal Service.[10] Arguably, however, there are unique aspects of the mail covers program that make it incompatible with the third-party doctrine, suggesting that the few decisions relying on this doctrine to uphold mail covers were wrongly decided.[11]

In addition, the third-party doctrine has itself been significantly undermined in recent years. Indeed, a majority of the Supreme Court now seems open to rejecting the doctrine in favor of new theories of Fourth Amendment jurisprudence that better balance the interests of

---

6. There is reason to believe the vast majority of these mail covers would be for separate individuals, given that extensions are available if a cover on a single individual needs to be continued. However, it is likely that a small subset are repeats. The USPS has not made available information that clarifies this point.

7. *See* Ron Nixon, *U.S. Postal Service Logging All Mail for Law Enforcement*, N.Y. TIMES (July 3, 2013), http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html?_r=0 [https://perma.cc/HN6T-ZDTS].

8. See, for example, *United States v. Choate*, 576 F.2d 165, 209 (9th Cir. 1978), discussed *infra* Part II.

9. The Fourth Amendment, enacted to protect citizens' homes and property from unwarranted government search, states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

10. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976) (along with *Smith v. Maryland*, establishing the third-party doctrine and solidifying its place in Fourth Amendment jurisprudence).

11. *See infra* Section II.B.1 (discussing, e.g., the governmental and monopolistic nature of the USPS, which leaves individuals with little choice but to turn over their mailing information).

law enforcement with the protection of citizen privacy in a modern, technological age.[12] One such theory, coined the "mosaic theory," essentially states that collecting mass amounts of data capable of revealing a detailed picture of an individual's life is an unreasonable—and thus unconstitutional—search, even where individual instances of more tailored data collection of the same kind would be allowed.[13] In other words, the mosaic theory cares less about the *process* used for information gathering and more about the *quantity and content* of the information gathered. It therefore challenges any technique capable of creating a detailed map—or "mosaic"—of a subject's daily activities without a warrant.

Put simply, the mosaic theory pushes back on the idea that individuals have no privacy rights whatsoever over the information they choose to reveal to third parties. In doing so, it seeks to reconceptualize the idea of a "reasonable expectation of privacy" in light of newly evolving societal and technological norms.[14] If adopted, the mosaic theory would consequently transform Fourth Amendment jurisprudence and open new avenues to challenge surveillance techniques, like mail covers, that are designed explicitly to develop a mosaic picture of a subject's cumulative communications.[15]

In order to consider this potential evolution of the Fourth Amendment from a new perspective, this Note examines the institutional and legislative history of the mail covers program—perhaps the first government surveillance initiative to track citizens' communications data. In doing so, it argues that the history of the program reveals two realities: first, that the government has a long-standing tendency to abuse broad surveillance initiatives and, second, that the Court's use of the third-party doctrine has rendered it incapable of combatting that abuse. The Note consequently employs mail covers as a case study through which to advocate for a change to Fourth Amendment jurisprudence. More specifically, it argues for the adoption of the mosaic theory and the implementation of a range of reforms to current standing and discovery laws that will better protect the long-neglected privacy rights of citizens.

---

12. *See* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 438–42 (2013).

13. *See, e.g.*, Erin Smith Dennis, Note, *A Mosaic Shield:* Maynard*, the Fourth Amendment, and Privacy Rights in the Digital Age*, 33 CARDOZO L. REV. 737, 738 (2011).

14. Katz v. United States, 389 U.S. 347, 351 (1967) (creating the "reasonable expectation of privacy" test).

15. *See* Benjamin M. Ostrander, Note, *The 'Mosaic Theory' and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733, 1750–51 (2011) (noting that the adoption of mosaic theory would call the validity of mail covers into question).

Part I provides a detailed examination of the history and inner workings of the mail covers program, aggregating data from a number of diverse sources to provide the only comprehensive scholastic analysis of the program in the modern era. Part II analyzes relevant Fourth Amendment law, culminating in an examination of the various challenges to the mail covers program that may exist under present and potential future versions of that law. Part III then proposes ways to reform both the mail covers program specifically and Fourth Amendment jurisprudence generally, with the goal of ensuring that privacy rights are taken seriously in an age of mass surveillance. Finally, the Note concludes by considering why such reform is necessary given the undeniable security benefits of mass surveillance in a world plagued by terrorism and cyber warfare.

Taken as a whole, this Note sheds new light on an area of surveillance law that has been largely overlooked despite its expansive influence on current surveillance initiatives. Perhaps most importantly, it also reveals that, even as far back as the 1970s, the potential for abuse inherent in government surveillance initiatives prompted courts to consider something like the mosaic theory as an alternative to the controversial third-party doctrine. In short, this Note exposes the fact that the need for change in Fourth Amendment jurisprudence existed long before Snowden's revelations made President Carter afraid to use email and, indeed, long before modern technology opened our eyes to the dangers of the surveillance initiatives that had been monitoring us all along.

I. THE USE AND ABUSE OF MAIL COVERS

A. A Brief History

The sole authority and procedure for establishing a mail cover and obtaining information from it derives from 39 C.F.R. § 233.3.[16] That regulation defines a mail cover as:

> [T]he 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.[17]

16. Mail Covers, 39 C.F.R. § 233.3(b) (2016).
17. § 233.3(c)(1).

Although these particular regulations were not implemented until 1975, mail covers have existed as an important investigative technique since at least 1879,[18] making them perhaps the first government surveillance technique designed to collect citizens' communications data.[19] Until the 1950s, however, the public remained unaware of the government's use of mail covers, and they were regularly implemented without any material restraints.[20] The recklessness of the McCarthy Era eventually changed that, and alerted the public that the government regularly abused the mail covers program. In 1952, it was revealed that a mail cover had been placed on Senator McCarthy himself at the request of an investigator on the Senate Subcommittee on Privileges and Elections.[21] That same year, the CIA implemented its New York mail intercept program, which began as a "proposal . . . to scan exteriors of all letters to the Soviet Union and to record, by hand, the names and addresses of the correspondents."[22] That program later evolved into "one of the most significant CIA mail opening programs" in history.[23] Both of these scandals led the Postal Service to reconsider its mail cover regulations in 1954 and add more specific requirements and procedures.[24]

Still, despite these new regulations, widespread use and abuse of the mail covers program continued. In 1964, the public discovered that the government had placed a cover on Roy Cohn, a prominent New York attorney facing perjury and conspiracy charges.[25] This discovery triggered public scrutiny of the program and widespread fear of unsupervised government surveillance.[26] In response, the Senate

18. United States v. Choate, 576 F.2d 165, 177 (9th Cir. 1978) (noting that the first postal regulations authorizing the use of mail covers were put forth in that year but also recognizing those regulations were likely implemented to regulate an already existing practice); *see also* KRIS & WILSON, *supra* note 4 ("Mail covers have been authorized since the late 1800s.").

19. *See* Nicole B. Cásarez, *The Synergy of Privacy and Speech*, 18 U. PA. J. CONST. L. 813, 836–37 (2016) ("[T]he protection of communications privacy in America originated not from judicial interpretations of the Constitution, but rather from early postal policies.").

20. *See Invasion of Privacy: Use and Abuse of Mail Covers*, 4 COLUM. J.L. & SOC. PROBS. 165, 166 (1968) [hereinafter *Invasion of Privacy*] (noting that the procedures regarding the use of mail covers in the 1950s "authorized virtually any government employee to obtain a cover upon anyone in the country, including Senators").

21. *Id.* at 165–66.

22. S. REP. NO. 94-755, at 567 (1976), http://www.aarclibrary.org/publib/church/reports/book3/html/ChurchB3_0287a.htm [https://perma.cc/Q7H3-EQ9J].

23. KRIS & WILSON, *supra* note 4.

24. *Invasion of Privacy*, *supra* note 20, at 166.

25. *Id.* at 170.

26. *Id.* ("Public belief that Attorney General Robert F. Kennedy was 'out to get' Cohn triggered adverse public response to the use of this unusual investigative procedure. Further, the incident brought to public attention the possibility that the government could monitor the mail of a private individual.").

Subcommittee on Administrative Practice and Procedure held public hearings on the matter in 1965.[27] Those hearings uncovered a startling "lack of central control over mail covers," and revealed that "at the time, there were approximately 1000 covers instituted per month, running for an average of two weeks each."[28] Such revelations led Senator Edward Long of Missouri, Chairman of the Subcommittee, to introduce a bill to abolish mail covers altogether.[29] In response, the Postal Service again revised its regulations, creating a "32-paragraph order" similar to the regulations now in place under 39 C.F.R. § 233.3.[30] While this quelled Senator Long's threats of abolishment, however, it did not end abuse of the program.[31]

Congress passed the first statutory regulations related to the mail covers program in 1975, after yet another public scandal brought attention to the inconsistency and unsupervised nature of the program when controlled by Postal Service regulations alone.[32] The scandal involved a sixteen-year-old student who wrote a letter to the Socialist Labor Party requesting information about its policies as part of an assignment for her high school social studies class.[33] Unfortunately, the student mistakenly addressed the letter to The Socialist Workers Party, whose mail the FBI was tracking, and inadvertently became the subject of an FBI investigation for "subversive" activities.[34] The investigation was extensive, even including a field investigation wherein an agent was dispatched to the student's school.[35] The mix-up became local and national news, prompting the creation and passage of the first version of 39 C.F.R. § 233.3. These regulations essentially parroted those implemented by the Postal Service after the public hearings in 1965, including a broad provision allowing a mail cover to be instituted in the interest of "protecting national security."[36] After the student sued and a district court determined that the "protecting national security" provision of the regulations was "unconstitutionally vague and

27. *Id.*; *Invasions of Privacy (Government Agencies)*: *Hearing Before the Subcomm. on Admin. Practice & Procedure of the S. Comm. on the Judiciary,* 89th Cong. 68 (1965).

28. *Invasions of Privacy*, *supra* note 20, at 170.

29. *Id.* at 172.

30. *Id.* at 173–74. A copy of these regulations, put forth in the Post Office Department's Weekly Postal Bulletin of June 17, 1965, can be found at http://www.uspostalbulletins.com/PDF/Vol86_Issue20478_19650617.pdf [https://perma.cc/TLK2-JN6S].

31. *Invasions of Privacy*, *supra* note 20, at 174–75 (noting continued abuse of the program throughout the late 1960s).

32. *See* Mail Covers, 39 C.F.R. § 233.3, WL 39 CFR § 233.3 (Westlaw through Pub. L. 104-208) (listing March 12, 1975 as the first amendment).

33. *See* Paton v. La Prade, 469 F. Supp. 773, 774–76 (D.N.J. 1978).

34. *Id.*

35. *Id.*

36. *See id.* at 779–81; KRIS & WILSON, *supra* note 4.

overbroad,"[37] however, the statute was modified in 1979 to include the following qualifications:

> Protection of the national security means to protect the United States from any of the following actual or potential threats to its security by a foreign power or its agents: (i) An attack or other grave, hostile act; (ii) Sabotage, or international terrorism; or (iii) Clandestine intelligence activities, including commercial espionage.[38]

Since that time—now over forty years ago—mail cover regulation has remained largely unchanged.

Unfortunately, the government's tendency to abuse the mail covers program has also remained unchanged. Although its secretive nature makes it difficult for individuals or watchdog groups to know when the government has inappropriately implemented a mail cover, documented instances of abuse—either in terms of a blatant disregard for 39 C.F.R. § 233.3's requirements, a use of the program for nefarious purposes outside the bounds established by § 233.3, or both—continue to emerge.

In the early 2000s, for example, a defense attorney in San Antonio learned that federal prosecutors had implemented a mail cover in order to track communications between the attorney and her client.[39] Although she complained about the blatant—and illegal[40]—abuse, the attorney never learned if the tracking stopped, and eventually lost the case.[41] Similarly, in 2011, a county supervisor in Arizona discovered that her mail was being tracked at the request of a sheriff whom she had openly criticized.[42] Calling the situation "a fishing expedition," the supervisor sued the county and eventually received a $1 million settlement that was affirmed by the U.S. Court of Appeals for the Ninth Circuit.[43] Finally, in 2012, a bookstore owner in Buffalo, New York learned his mail was being tracked after he mistakenly received a confidential notice intended for postal workers, ordering them to show his mail to Postal Service supervisors "for copying" prior to delivery.[44] While the man had been part of the radical Earth Liberation Front

37. *Paton*, 469 F. Supp. at 782.

38. Mail Covers, 39 C.F.R. § 233.3(c)(9) (2016).

39. Ron Nixon, *Report Reveals Wider Tracking of Mail in U.S.*, N.Y. TIMES (Oct. 27, 2014), http://www.nytimes.com/2014/10/28/us/us-secretly-monitoring-mail-of-thousands.html?_r=0 [https://perma.cc/B4Z6-ETK2].

40. § 233.3(g)(3) ("No mail cover shall include matter mailed between the mail cover subject and the subject's known attorney.").

41. Nixon, *supra* note 39.

42. *Id.*

43. *Id.*

44. Nixon, *supra* note 7. A secondary link, available at http://www.nytimes.com/interactive/2013/06/30/us/30postal-mail-cover-documents.html [https://perma.cc/DXA8-ZXHH?type=image], provides the notice.

activist group in the early 2000s, had written books sympathetic to the liberation movement, and had occasionally invited politically radical speakers to his bookstore, he had not been actively involved in radical activism for many years by the time the mail cover was apparently implemented.[45] Each of these instances suggests ongoing abuse of the mail cover program.

The sheer magnitude of the program in the modern age also suggests abuse, abuse that the Postal Service itself has—to some extent—admitted. In 2014 alone, the USPS processed over 57,000 mail covers,[46] and an audit of the mail covers program revealed "systemic failures in authorization and monitoring."[47] Such failures are exemplified by the incredibly low rate of mail cover requests rejected by the Postal Service. From 2010 to 2014, only 341 mail cover requests were denied, while a total of 158,543 were granted.[48] This is a rejection rate of only two-tenths of a percent. Of the mail cover requests granted, the audit revealed that over twenty percent had not been properly approved and over ten percent had not been "adequately justified."[49] Additionally, "928 mail covers [were found to be] in active status even though their cover periods had ended."[50] In sum, the government has consistently abused the mail covers program throughout the program's history—and that abuse continues today.

B. Continued Use, Abuse, and Expansion

Unfortunately, the obvious systemic abuses detailed above have neither encouraged renewed reforms of the mail covers program nor

45. *Id.* The man, Leslie Pickering, recently filed suit against the USPS and the Transportation Security Administration, alleging that they withheld information owed to him under the Freedom of Information Act. He lost on summary judgement. *See* Pickering v. U.S. Dep't of Justice, No. 13–CV–00674A(F), 2015 WL 1458089, at *12 (W.D.N.Y. Feb. 25, 2015).

46. Office of the Inspector General, *U.S. Postal Inspection Service Mail Covers Program—Phase II Audit Report*, U.S. POSTAL SERV. 13 (Sept. 15, 2015), https://www.uspsoig.gov/sites/default/files/document-library-files/2015/hr-ar-15-007_0.pdf [https://perma.cc/6TLT-FCSP] [hereinafter *USPS Phase II Audit Report*].

47. Steven R. Morrison, *Mail Cover Surveillance: Problems and Recommendations*, NAT'L ASS'N CRIM. DEF. LAW. 3 (2015), https://www.nacdl.org/WorkArea/DownloadAsset.aspx?id=37034&libID=33173 [https://perma.cc/Y7DU-FW2K]; Office of the Inspector General, *Postal Inspection Service Mail Covers Program Audit Report*, U.S. POSTAL SERV. 1–2 (May 28, 2014), https://www.uspsoig.gov/sites/default/files/document-library-files/2015/hr-ar-14-001.pdf [https://perma.cc/8VTY-TZUF] [hereinafter *USPS Phase I Audit Report*]; *see also* Josh Gerstein, *Audit: Snooping Safeguards Not Kept*, POLITICO (June 19, 2014, 8:58 AM), http://www.politico.com/story/2014/06/snail-mail-snooping-safeguards-not-followed-108056 [https://perma.cc/VZ3W-L3RD].

48. *USPS Phase II Audit Report*, *supra* note 46, at 13, 17.

49. *USPS Phase I Audit Report*, *supra* note 47, at 2.

50. *Id.*

discouraged attempts to expand it. After the devastation of the terrorist attacks on September 11, 2001, the Bush Administration endeavored to amend mail cover regulations to give the FBI unfettered discretion to determine when mail covers should be issued: "The plan would effectively eliminate the postal inspectors' discretion in deciding when so-called mail covers are needed and give sole authority to the Federal Bureau of Investigation, if it determines that the material is 'relevant to an authorized investigation to obtain foreign intelligence . . . .' "[51] As the shockingly low rate of rejections noted above makes plain, this was in large respect only a codification of the status quo,[52] albeit one that certainly pushed the boundaries of the "national security" prong of 39 C.F.R. § 233.3 once again.[53] Still, the plan was harshly criticized by civil rights advocates and never enacted into law.[54]

The Bush Administration was successful, however, in implementing two programs that, while not mail cover operations themselves, have drastically enhanced the surveillance capabilities of the Postal Service. Together, the Mail Imaging program and the Mail Isolation Control and Tracking program allow the Postal Service to "photograph the exterior of every piece of paper mail that is processed in the United States."[55] That amounts to a record of roughly 160 billion mail parcels every year.[56] Both programs were allegedly implemented to help sort mail and investigate suspicious packages.[57]

The USPS claims that the Mail Imaging program has been in use since the early 1990s,[58] while the Mail Isolation Control and Tracking program began in 2001 after anthrax attacks claimed five

51. Eric Lichtblau, *Plan to Let F.B.I. Track Mail in Terrorism Inquiries*, N.Y. TIMES (May 21, 2005), http://www.nytimes.com/2005/05/21/politics/plan-to-let-fbi-track-mail-in-terrorism-inquiries.html?_r=0 [https://perma.cc/LCZ8-SD8N].

52. *See also id.* (noting that postal officials have reported that "the Postal Service had not formally rejected any requests from the [FBI] in recent years").

53. *See* discussion regarding the 1979 modifications to section 233.3, addressed *supra* Section I.A.

54. *See* KRIS & WILSON, *supra* note 4; Lichtblau, *supra* note 51.

55. Nixon, *supra* note 39; Nixon, *supra* note 7.

56. *Postal Facts*, U.S. POSTAL SERV. 2 (2015), https://about.usps.com/who-we-are/postal-facts/postalfacts2015.pdf [https://perma.cc/MSH6-DHPQ].

57. These photographs are now also being used to provide consumers of mail with a digital preview of their daily mail via the Informed Delivery program. *See* Herb Weisbaum, *New USPS Service Lets You Digitally Preview that Day's Mail Delivery*, NBC NEWS (Apr. 3, 2017, 7:32 AM), http://www.nbcnews.com/business/consumer/new-usps-service-lets-you-digitally-preview-day-s-mail-n741926 [https://perma.cc/M5XX-DDER].

58. Lauren Walker, *Postal Service Photographs Every Piece of Mail in the U.S., Shares with Agencies that Request It*, NEWSWEEK (Oct. 28, 2014, 4:47 PM), http://www.newsweek.com/postal-service-photographs-every-piece-mail-us-shares-agencies-request-it-280614 [https://perma.cc/K8BM-VQGV]. See the "update" at the bottom, including a response letter from USPS.

lives, including two postal workers.[59] Neither program was publicly known until 2013, however, when investigations relating to ricin-laced letters mailed to President Obama and Mayor Michael Bloomberg revealed their existence.[60] Since then, very little has been disclosed about these programs. In a 2013 interview, then-Postmaster General Patrick Donahoe noted that the images collected are not housed in any single location, but are generally stored "for between a week and 30 days and then disposed of."[61] He went on to state that the programs have been used by law enforcement "a couple of times."[62] However, no evidence has been provided to back up these claims, no other government official appears to have ever addressed the programs, and no information about the management, intricate workings, or regulations of the programs has been made publicly available.

While not directly related to mail covers, these programs reveal the extent to which mail surveillance has grown in recent years without renewed oversight.[63] As cybersecurity expert Mark Rasch put it,

> In the past, mail covers were used when you had a reason to suspect someone of a crime. Now it seems to be "Let's record everyone's mail so in the future we might go back and see who you were communicating with." Essentially you've added mail covers on millions of Americans.[64]

While this may be hyperbole,[65] the history of the mail covers program is undeniably one wrought with a lack of oversight and consistent abuse. This should concern the public for many reasons, not least of which is simply how much information mail covers allow the government to uncover. After implementing a cover, the government can easily divine an individual's entire social network—including the names and addresses of friends and family—along with critical

59. Nixon, *supra* note 7.

60. *Id.*

61. Andrew Miga, *AP Interview: USPS Takes Photos of All Mail*, ASSOCIATED PRESS (Aug. 2, 2013, 12:41 AM), http://www.sandiegouniontribune.com/sdut-ap-interview-usps-takes-photos-of-all-mail-2013aug02-story.html [https://perma.cc/64GZ-Z5N2].

62. *Id.*

63. The nearly exponential expansion of the mail covers program itself does the same. In 1975, when the last significant regulations were passed, only 3,699 mail covers were issued while 191 were disapproved, a rejection rate of five percent. See the concluding paragraph to Section I.A to compare with the 57,000 mail covers and .02 percent rejection rate of 2014. The relatively high rejection rate of 1975 is no doubt due in large part to Congress's interest in the program as it was passing regulations. The fact that the program has grown so much since then with no new regulations or significant hearings shows a renewed sense of apathy toward the program that has allowed abuse to repeatedly surface. *See* United States v. Choate, 576 F.2d 165, 188 n.18 (9th Cir. 1978) (citing mail cover disapprovals and approvals for 1973–1975).

64. *See* Nixon, *supra* note 7 (quoting Rasch).

65. Without more information, we really cannot know how these programs are being used.

banking, business, and political information.[66] For example, there is no limitation preventing the government from using mail covers to surveil mailing lists sent out by schools, corporations, or other organizations. Members of politically contentious organizations that may pose any vague threat to "national security" under 39 C.F.R. § 233.3's guidelines can thus be easily uncovered, and connections within such organizations exposed.

Additionally, because the government also investigates the senders and receivers of a subject's mail,[67] the rights of "large numbers of citizens" beyond those whose mail is actually being tracked are implicated in mail cover investigations.[68] Finally, in the modern age of online shopping, mail covers allow government agencies to know not only when an individual has received a package but also, given the relative sizes of packages and return addresses often adorned with descriptive organization names, a good idea of what is inside. Together, these connections can reveal a very descriptive picture of an individual's network and daily life. This information is all gathered without a search warrant or, indeed, judicial review of any kind.

To request a mail cover, a law enforcement agent need do little more than fill out a standardized form.[69] Once granted, a mail cover remains in effect for thirty days, although it can be extended for up to 120 days with "adequate justification," and even that 120-day limit can be extended with additional approval from the Chief Postal Inspector

---

66. *See, e.g.*, Nixon, *supra* note 7 (quoting former F.B.I. operative James J. Wedick as follows: "Looking at just the outside of letters and other mail, I can see who you bank with, who you communicate with—all kinds of useful information that gives investigators leads that they can then follow up on with a subpoena."); *see also Choate*, 576 F.2d at 187:

> It is possible to learn the identities, addresses and frequency of contact of most of a person's correspondents through a one-month mail cover including banks, creditors, affiliations with religious, political, educational, and voluntary organizations, publications received, accountants, and friends. Because many of these correspondents maintain files on the addressee which can be discovered and used by the investigating agency . . . the mail cover used in combination with other techniques quickly makes the subject's life an open book to investigators. (citation omitted).

67. *See supra* Section I.A (discussing how the government opened investigations on any person who sent a letter to the Socialist Workers Party). Also see *Lustiger v. United States*, 386 F.2d 132 (9th Cir. 1967) and *United States v. Schwartz*, 283 F.2d 107 (3d Cir. 1960), in which the Post Office contacted everyone who had corresponded with mail fraud suspects, and *United States v. Leonard*, 524 F.2d 1076 (2d Cir. 1975), in which the Post Office investigated everyone who received mail from Switzerland without a return address.

68. *Choate*, 576 F.2d at 188 (Hufstedler, J., dissenting).

69. *See* Nixon, *supra* note 7 ("For mail cover requests, law enforcement agencies submit a letter to the Postal Service, which can grant or deny a request without judicial review."). To see the standardized form used, see *USPS Procedures: Mail Cover Requests*, U.S. POSTAL INSPECTION SERV. (March 2006), https://cryptome.org/isp-spy/usps-spy.pdf [https://perma.cc/UFF6-HQ2T], also available as an interactive document at the secondary link listed *supra* note 44.

or his agents.[70] It has not been reported how often such extensions are requested or granted; a 2014 audit reported that extensions were often inadvertently and inappropriately granted automatically due to a lack of oversight of mail cover system controls, suggesting that the initial thirty-day limit may be startlingly flexible.[71] The low rate of rejections in initial grants of mail covers, noted above, also implies that Postal employees often defer to the discretion of requesting agencies, suggesting that a similarly low rate of extension rejections is likely.[72] Once completed, information obtained from a mail cover is retained for eight years, three years beyond the retention of national security-related telephony metadata.[73] It is unclear if any of these limitations—or, indeed, any limitations at all—have been applied to the newer mail imaging programs.

In short, mail covers are remarkably easy for the government to obtain and only minimally restricted by limitations that appear to be rarely followed, despite the long history of abuse inherent in the mail covers program and the breadth of information it is capable of collecting and retaining. As such, and in light of the current public discourse regarding data privacy, it may be time to reconsider the program. At least as far as courtroom challenges go, changing Fourth Amendment jurisprudence may provide an opportunity to do just that.

II. CHALLENGES AND CHANGES IN THE COURTROOM

The most important case so far challenging the validity of mail covers is *United States v. Choate*.[74] There, a defendant charged with income tax evasion challenged the constitutionality of the Federal Bureau of Customs' use of a mail cover to uncover the name of a bank with which he had an account—a fact that became crucial to the

70. Mail Covers, 39 C.F.R. § 233.3(g)(6) (2016); Morrison, *supra* note 47, at 6; *USPS Phase II Audit Report*, *supra* note 46, at 6.

71. *USPS Phase I Audit Report*, *supra* note 47, at 6:

> Attempts to extend a mail cover past its original end date resulted in an error message being displayed in the ISIIS, indicating the mail cover had already been extended. Further, an error in the ISIIS mail cover application sometimes allowed the same mail cover tracking number to be assigned to different mail cover requests. This occurred because management did not ensure system control features, such as integrity checks, were operating as designed.

72. *See supra* the concluding paragraph to Section I.A (discussing mail cover rejection rates). The fact that the bookstore owner discussed *supra* Section I.A was being tracked years after being involved in arguably subversive activities is further evidence that mail covers may be lasting far longer than intended under 39 C.F.R.§ 233.3.

73. § 233.3(h)(4); Morrison, *supra* note 47, at 23.

74. 576 F.2d 165 (9th Cir. 1978).

Internal Revenue Service's case against him.[75] The defendant claimed that the mail cover constituted an illegal search under the Fourth Amendment because it violated his "reasonable expectation of privacy."[76]

This "reasonable expectation of privacy" test was first articulated in *Katz v. United States*, wherein the Supreme Court exchanged its prior, property-based approach to Fourth Amendment jurisprudence for "the concept that 'the Fourth Amendment protects people, not places.' "[77] In so indicating that "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure," the Supreme Court opened the door to new Fourth Amendment challenges, including those introduced in *Choate*.[78] Whereas only a month prior to *Katz*, the Ninth Circuit had casually written off mail covers as conclusively constitutional,[79] the post-*Katz* landscape now allowed for the (ultimately unsuccessful) argument that an "overbroad" search could be unreasonable, even where it was conducted "in an area in which [the subject had] neither a property interest, nor any personal stake or claim," such as a Post Office.[80] Thus, *Choate* became the only case to substantially question the validity of the domestic mail covers program under the Fourth Amendment—and the *Choate* court very nearly ruled against the program's constitutionality.[81]

---

75. *Id.* at 168.

76. *Id.* at 174–75.

77. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT, § 2.7(a) (5th ed.) (citing Katz v. United States, 389 U.S. 347, 351 (1967)).

78. *Katz*, 389 U.S. at 353.

79. *See* Lustiger v. United States, 386 F.2d 132, 139 (9th Cir. 1967) (relying on earlier mail cover cases that had not considered constitutionality to casually assert that "the Fourth Amendment does not preclude postal inspectors from copying information contained on the outside of sealed envelopes in the mail, where no substantial delay in the delivery of the mail is involved"). The cases relied upon in *Lustiger* were *Cohen v. United States*, 378 F.2d 751 (9th Cir. 1967), *United States v. Schwartz*, 283 F.2d 107 (3d Cir. 1960), and *United States v. Costello*, 255 F.2d 876 (2d Cir. 1958), all of which involved violations or obstructions of mail or postal regulations and failed to even mention the Fourth Amendment. *See Choate*, 576 F.2d at 195–96.

80. *Choate*, 576 F.2d at 184, 199 (Hufstedler, J., dissenting). Note that *Lustiger* was also distinguishable from *Choate* in that the defendant there was charged with mail fraud rather than a crime unrelated to the mail, as in *Choate*. *See id.* at 196 n.46.

81. The Second Circuit considered a case similar to *Choate* with its decision in *United States v. Leonard*, 524 F.2d 1076 (2d Cir. 1975), which "involved use of a mail cover to monitor all incoming air mail from Switzerland without return addresses." *Choate*, 576 F.2d at 197 (Hufstedler, J., dissenting). However, as noted by Justice Hufstedler in *Choate*, *Leonard* involved international mail that fell "within the rationale of the 'border search' exception to the warrant clause of the Fourth Amendment," and could not be controlling with respect to domestic mail covers. *Id.* at 198 (Hufstedler, J., dissenting). Thus, *Choate* remains the most—and perhaps only—relevant case in discussions of the domestic mail cover program.

This Part analyzes the evolution of the Fourth Amendment as it relates to different theories of the constitutionality of mail covers—or lack thereof. Section A considers the presently controlling third-party doctrine and suggests that the underpinnings of this controversial doctrine have been significantly undermined in recent years. It then moves on to discuss the more privacy-friendly mosaic theory as a potential successor to the third-party doctrine in Fourth Amendment-focused surveillance cases. Section B analyzes the fate of the mail covers program under the various iterations of Fourth Amendment law discussed in Section A, revealing a wide range of potential challenges to the program's constitutionality.

A. The Modern Fourth Amendment

1. The Third-Party Doctrine

As noted above, *Choate* involved a tax evasion scandal brought to light in part through the use of a mail cover. In a 2-1 decision, the Court of Appeals for the Ninth Circuit reversed the decision of the district court and ruled against the defendant, relying on what would come to be known as the "third-party doctrine" of Fourth Amendment jurisprudence.[82] This doctrine states that an individual cannot claim a "reasonable expectation of privacy" under *Katz* over information she has willingly revealed to a third party.[83] Thus, in *Choate*, the defendant could not claim that the mail cover violated his reasonable expectation of privacy: because he had willingly revealed the mailing information exposed by the mail cover to the USPS in exchange for mailing services, he had assumed the risk that the USPS, as a third party, would turn that information over to government authorities at any time.

The third-party doctrine had not been fully solidified as a basic tenet of Fourth Amendment law at the time *Choate* was decided. Nonetheless, the Ninth Circuit majority applied the doctrine, relying on precedent established in *United States v. White*, a 1971 Supreme Court case that determined individuals have no reasonable expectation of privacy over conversations disclosed in presumed confidence with undercover informants.[84] It also relied on *United States v. Miller*, a 1976 Supreme Court case holding that individuals have no reasonable expectation of privacy over original checks and deposit stubs they

82. *Choate*, 576 F.2d at 165.

83. *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976) (along with *Smith v. Maryland*, establishing the third-party doctrine and solidifying its place in Fourth Amendment jurisprudence).

84. 401 U.S. 745, 752–53 (1971).

voluntarily convey to banks.[85] Drawing on this precedent, the *Choate* court reasoned that

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[86]

In other words, the court applied the third-party doctrine and denied defendant Choate's motion to suppress the evidence collected as a result of his mail cover.

Just a year after *Choate*, the Supreme Court confirmed the third-party doctrine as a key aspect of Fourth Amendment jurisprudence with its decision in *Smith v. Maryland*.[87] There, the Court applied the doctrine to pen registers, a surveillance technique wherein a device is attached to a telephone line and used to covertly record the outgoing numbers called from the line.[88] Echoing the language of the *Choate* majority, the *Smith* majority concluded:

> This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.[89]

Put differently, the Court applied the third-party doctrine to find that the defendant could not reasonably expect to keep private data he had

---

85. 425 U.S. 435, 442–43 (1976).

86. *Choate*, 576 F.2d at 175. The majority also very briefly stated that the information on the outside of an envelope may be considered in plain view, subject to search and seizure at will. *See id.* at 174–80. In response, Judge Hufstedler noted in dissent that such information is not suspicious or remarkable in and of itself and thus, under the plain view tests established in *Coolidge v. New Hampshire*, 403 U.S. 443, 464–73 (1971), "falls within the set of cases as to which obtaining a warrant will present no substantial problem and for which plain view offers no justification." *Choate*, 576 F.2d at 204 (Hufstedler, J., dissenting). The case law surrounding the plain view doctrine—which unanimously requires police officers to have a prior, probable cause-supported justification to collect evidence before allowing them to obtain incriminating items found in plain view—supports Judge Hufstedler's arguments. *See Coolidge*, 403 U.S. at 466. The case law surrounding mail covers also seems to agree with Judge Hufstedler, as it rarely even mentions the plain view doctrine. Indeed, even the basic argument that mail parcels are in plain view is weak, given that such parcels move directly from mail boxes to USPS custody and back again. *See infra* Section II.B.1 (noting that the USPS has been characterized as a bailee of mail parcels, with duties to privately carry and deliver parcels). For all of these reasons, this Note will not address the plain view argument in depth.

87. 442 U.S. 735 (1979).

88. Other information collected by pen registers includes basic information about the telephone line, such as "the number of times [the] telephone rings when incoming calls are received." Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 17 (2003). A "pen register does not indicate whether anyone answers the outgoing [or incoming] call" and does not "monitor [or] record the content of telephone conversations." *Id.*

89. *Smith*, 442 U.S. at 744.

freely chosen to share, even if he shared it only with a phone company and only for the limited purpose of connecting a call.

In many regards, this reasoning makes sense. The point of the third-party doctrine is, after all, to accommodate the choices of individuals regarding which information they choose to keep absolutely private and which information they are comfortable sharing, at least in some capacity, with others. Why should the government have the burden of determining for itself which information should be privileged—i.e., when a reasonable expectation of privacy exists—when it can simply take its citizens at their word? The third-party doctrine creates a clear, bright line rule for law enforcement that allows citizens to decide for themselves when to sacrifice efficiency for privacy. It also collects only noncontent data—what we now call "metadata"—so as to protect freedom of speech and discussion, ensuring that the actual content of conversations will not be obtained without a warrant.[90] When technology was rudimentary, much of this data was available to law enforcement via ordinary surveillance mechanisms; the third-party doctrine simply evens the playing field in an age where third-party mechanisms of communication are so easily available to criminals. Viewed in this light, it is a fair and necessary canon of Fourth Amendment law.[91]

There are, however, many other considerations in play when it comes to the third-party doctrine, especially given the now-dominant role technology plays in daily life. One can no longer feasibly live as an active and engaged citizen without frequently relying on third parties such as internet and cell phone service providers. When the alternative is effectively social isolation, the idea that anyone *voluntarily* conveys their information to these third parties has become even more of a legal fiction today than it was when *Smith* was decided.[92] Along the same lines, the argument that metadata is not excessively revealing is no longer convincing given that a significant portion of our interactions are

90. Note that the content/noncontent distinction so prevalent in surveillance law is not parodied in other aspects of Fourth Amendment jurisprudence. Even in *United States v. Miller*, discussed *supra* note 85 and accompanying text, the Court allowed suspicionless access to the "content" of the bank records in question. *See* 425 U.S. at 442. Thus, this argument in favor of the third-party doctrine is not relevant in all cases where the doctrine could be applied. I am indebted to Professor Christopher Slobogin for pointing this out.

91. For an excellent summary of the positives and negatives of the third-party doctrine, see Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, ABA J. (Aug. 1, 2012, 9:20 AM), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/ [https://perma.cc/MX3T-WLEN].

92. *See, e.g.*, Steven M. Bellovin, Matt Blaze, Susan Lanau & Stephanie K. Pell, *It's Too Complicated: How The Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, HARV. J.L. & TECH. (forthcoming 2017), https://ssrn.com/abstract=2791646 [https://perma.cc/7GPS-W2LC].

now electronic. Each time we virtually connect with someone, we leave behind a string of metadata that, taken cumulatively, essentially becomes a "relationship database."[93] As scholars have argued, "Big Data collection and the ready availability of personal data—peoples' GPS locations, Facebook likes, etc.—are now pervasive, even ubiquitous sources of information, most often in the possession of private companies offering consumers all kinds of IP-based services and products."[94]

The fact that metadata is particularly difficult to encrypt or otherwise keep private compounds this problem, because it leaves individuals with no substantive way to keep their virtual activities or conversations out of the government's reach.[95] Consequently, it no longer makes sense to equate modern, nearly omniscient surveillance initiatives with the rudimentary surveillance initiatives of the past, so prone as they were to human error and evasion. As Justice Douglas opined in his dissent in *United States v. White* back in 1971: "What the ancients knew as 'eavesdropping,' we now call 'electronic surveillance'; but to equate the two is to treat man's first gunpowder on the same level as the nuclear bomb."[96] The sentiment has never been more true.

All of this suggests that the third-party doctrine is not compatible with modern technological developments. As a result, many courts have begun rethinking their application of the third-party doctrine to surveillance cases. Indeed, even some members of the Supreme Court now appear willing to embrace new theories of Fourth Amendment jurisprudence better equipped to address the realities of the modern technological landscape. The most prevalent of these new

---

93. *See* Matt Blaze, *Phew, NSA is Just Collecting Metadata. (You Should Still Worry)*, WIRED (June 19, 2013, 9:30 AM), https://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/ [https://perma.cc/C6FB-DR7V].

94. Bellovin et al., *supra* note 92, at 9; *see also id.* at 9 n.35 (citing C. Jernigan & B. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, FIRST MONDAY (Oct. 5, 2009), http://journals.uic.edu/ojs/index.php/fm/article/view/2611/2302 [https://perma.cc/9CFF-KVDC] to note that "social graphs, likes, etc., can be quite revelatory of an individual's characteristics, even when these are not explicitly revealed"). I would add that the variety of apps now available and used for nearly every facet of life—consider, e.g., dating apps, exercise apps, transportation apps, and money transfer apps—can reveal a startlingly accurate picture of an individual's daily life.

95. Blaze, *supra* note 93:

> Content can be protected, somewhat inconveniently yet effectively enough, with encryption. But we leave trails of metadata everywhere, anytime we reach out to another person. And while there are techniques (such as Tor) that can defeat metadata traffic analysis under some circumstances, they don't cover all the ways we communicate.

96. 401 U.S. 745, 756 (1971) (White, J., dissenting); *see also supra* note 84 and accompanying text (discussing *White*).

theories, introduced in the 2012 Supreme Court case *United States v. Jones*,[97] will be discussed in the next Section.

2. The Mosaic Theory

In *Jones*, the Court unanimously held that the government could not, without a warrant, attach a Global Positioning System ("GPS") tracking device to defendant Jones's car in order to record his movements in that car twenty-four hours a day for a period of twenty-eight days.[98] The Justices were split, however, in their reasoning. Writing on behalf of a five-Justice majority, Justice Scalia reinvigorated the pre-*Katz* property-based approach to Fourth Amendment jurisprudence, arguing that the warrantless attachment of the GPS device to Jones's physical property—his car—constituted an unlawful trespass.[99] By deciding the case on these narrow grounds, the Scalia majority evaded the *Katz* "reasonable expectation of privacy" test altogether, leaving the third-party doctrine unchanged.[100]

In contrast, a four-Justice concurrence written by Justice Alito, along with a solo concurrence penned by Justice Sotomayor, took on the third-party doctrine more directly, considering it in light of a new theory of Fourth Amendment jurisprudence introduced by the U.S. Court of Appeals for the District of Columbia in its lower-court opinion.[101] This "mosaic theory" embraces the notion that individually constitutional searches may become unreasonable under the Fourth Amendment when cumulatively collected.[102] As the D.C. Circuit argued: "Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what a person does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation."[103]

Justice Alito, while not explicitly referencing the mosaic theory, clearly implicated its reasoning in his *Jones* concurrence, wherein he opined that while "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable[,] . . . the use of longer term

97. 565 U.S. 400 (2012).

98. *Id.* It was actually his girlfriend's car, but that fact is not relevant to this discussion.

99. *Id.* at 404–13.

100. *Id.*; *see also* Henderson, *supra* note 12, at 449.

101. *Jones*, 565 U.S. at 413–31.

102. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010); *see also* Smith Dennis, *supra* note 13.

103. *Maynard*, 615 F.3d at 562.

GPS monitoring in investigations of most offenses impinges on expectations of privacy."[104] Alito essentially argued that the government could use a GPS device to track a vehicle in a small number of individual instances, but not to the point where all of those individual instances combined to create a nearly complete picture of the subject's daily life.[105] In his view—and the views of the three other Justices who joined his opinion—the use of data to create such a comprehensive picture of an individual's daily activities goes far beyond what any reasonable citizen would expect of the government, and is consequently unconstitutional under *Katz*.[106] While not an explicit attack on the third-party doctrine, such reasoning implies that sweeping instances of surveillance that society is unwilling to recognize as reasonable will be unconstitutional, regardless of the subject's decision to turn over information to a third party or, as in *Jones*, avail herself of public amenities any third party could be observing.

In her solo concurrence, Justice Sotomayor tackled the third-party doctrine more directly, asserting:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[107]

In other words, Sotomayor acknowledged the enhanced role of third parties in the modern world and, consequently, questioned the third-party doctrine's assumption of voluntary conveyance.[108]

In Justice Sotomayor's view, this voluntariness issue could be solved if the Court were to adjust the *Katz* analysis to take into account the particular capabilities of the surveillance mechanism in question.[109] This approach is different—and arguably more expansive—than Justice Alito's, because it focuses on the objective power of surveillance mechanisms rather than the societal expectations associated with those mechanisms, which are capable of changing as technology does. As Professor Orin Kerr summarized:

> Justice Alito's opinion [in *Jones*] focused on surprise. It looked to whether the investigation exceeded society's expectations for how the police would investigate a particular crime. In contrast, Justice Sotomayor's approach looked to whether police

104. *Jones*, 565 U.S. at 430 (Alito, J., concurring).

105. *Id.*

106. *Id.*

107. *Id.* at 417 (Sotomayor, J., concurring).

108. Sotomayor's view here harkens back to a long line of cases questioning the voluntariness prong of the third-party doctrine. *See, e.g.*, discussions *supra* pp. 1643–44 and *infra* Section II.B.1.

109. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

> conduct collected so much information that it enabled the government to learn about a person's private affairs "more or less at will."[110]

Regardless, the bottom line is that, even if they have slightly different views as to how the mosaic theory—or something like it—should be implemented, many Justices on the Supreme Court now seem open to the idea of evolving the *Katz* framework away from the third-party doctrine in future cases, and even the Justice Scalia majority was not openly opposed to doing so.[111]

This openness to a significant expansion of privacy protections in Fourth Amendment jurisprudence could mark a turning point in constitutional law. As described *infra*,[112] this change has been long in the making, but it has the power to open up new realms of constitutional challenges. The mail covers program provides a particularly apt example of what these new challenges could be and where Fourth Amendment law stands today. As such, the next Section will examine potential challenges to the mail covers program under each of the two primary doctrines of Fourth Amendment jurisprudence in play in the post-*Jones* landscape: the currently dominating third-party doctrine and the emerging mosaic theory doctrine.

---

110. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 328 (2012) (citing *Jones*, 565 U.S. at 956 (Sotomayor, J., concurring)).

111. We will soon have a better idea of exactly where the Justices stand on this issue and whether they intend to adopt the mosaic theory in Fourth Amendment cases involving the collection of cumulative communication or location data. At the time of publication, the Court has granted certiorari in *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017), a case questioning the government's acquisition of certain "transactional records" from defendant's cellphone service provider. Those records included the numbers dialed and received from defendant's cellphone, as well as cell-site information detailing the locations from which defendant began and ended his calls over a period of 127 days. 819 F.3d at 884. Citing the third-party doctrine and the noncontent nature of the information at issue, the Sixth Circuit in *Carpenter* rejected defendant's arguments that the government's search of such data required probable cause. *Id.* at 886–90. In doing so, however, the Sixth Circuit was careful to distinguish *Carpenter* from *Jones*, comparing the trespass that occurred in *Jones* with the relatively benign collection of business records in *Carpenter*, and comparing the accuracy of the GPS data collected in *Jones* with the relative inaccuracy of locational data obtained from the cell-site information in *Carpenter*. *Id.*

The Supreme Court's decision in *Carpenter* will undoubtedly shed new light on the Court's desire, or lack thereof, to evolve the Fourth Amendment. It could also significantly impact the arguments presented in this Note. Still, the unique aspects of the mail covers program that make it unconstitutional under *either* the third-party doctrine *or* the mosaic theory—see *infra* Section II.B—will remain unchanged regardless of the outcome in *Carpenter* and, indeed, would be significantly strengthened were the Court to reverse the Sixth Circuit in *Carpenter* and find that an illegal search had occurred.

112. Section II.B (explaining that the third-party doctrine has been undermined in recent years and revealing that even as far back as 1978 some judges were open to applying the mosaic theory in surveillance cases).

B. Mail Covers and the Post-Jones Landscape

1. The Third-Party Doctrine, Revisited

It is worth reiterating that the Supreme Court has never taken up a mail cover challenge, and that *Choate* may have been wrongly decided even with a strong third-party doctrine intact. Indeed, in response to the majority's third-party assertions in *Choate*, both district court Judge Ferguson and dissenting appellate Judge Hufstedler made compelling arguments against the third-party doctrine in their opinions, attacking it both generally and specifically in relation to mail covers. Further, many of these arguments have since been supported by Supreme Court precedent that significantly undermines the underpinnings of the third-party doctrine.

For his part, district court Judge Ferguson considered the reasonability of the defendant's expectation of privacy over his mail, noting:

> It cannot be denied that a reasonable person's expectation of privacy with regard to return addresses on mail is a somewhat limited one. He understands that this information is necessary to postal operations and will be examined and utilized in order to route items when the name and address of the addressee is incorrect, absent, or illegible. But the disclosure mandated by these circumstances is not broad or for all purposes: a reasonable person still expects (1) that the information contained in the return address will only be used for postal purposes, and (2) that it will be utilized in only a mechanical fashion without any records being kept. The recording and disclosure to non-postal authorities for non-postal purposes that results from a mail cover extends far beyond these narrow bounds.[113]

Here, Judge Ferguson challenges the notion, embraced within the third-party doctrine, that each time a reasonable person expects—or even intends—a third party to observe some of her information for certain specified purposes, that person should expect the third party to record the information. Instead, Judge Ferguson argues that privacy need not be an all-or-nothing inquiry: in the context of mail covers, for example, an individual can willingly turn over the information on the outside of her mail for the explicit purpose of delivery while still maintaining a privacy interest over that information as it relates to all other purposes.

This idea that privacy is not absolute has gained traction in light of Supreme Court precedent questioning the narrow conception of what constitutes a reasonable expectation of privacy under the third-party doctrine. In the 2001 case *Ferguson v. City of Charleston*, for example, the Court found a Fourth Amendment violation when a state hospital obtained and tested urine samples from its pregnant patients and gave

113. United States v. Choate, 422 F. Supp. 261, 270 (C.D. Cal. 1976).

the results to the police, who then arrested the patients and sought to assist them in receiving drug treatment.[114] As the dissent noted,[115] this was a departure from the Court's precedent involving undercover informants—particularly its assertion in *Miller* that the third-party doctrine applies "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[116] The departure suggests the Court's willingness to find certain processes of data collection to be so invasive as to be unreasonable, even if a robust third-party doctrine would support their constitutionality. This potentially bolsters Judge Ferguson's more expansive conception of privacy rights.

In his district court opinion in *Choate*, Judge Ferguson went on to explain that an expansive conception of privacy rights was particularly warranted in the case of mail covers because of the governmental and monopolistic nature of the USPS. In his words:

> [T]he fact that the Postal Service is a government-sanctioned monopoly cannot be ignored . . . [T]here are few alternatives to the mail. Surely, in a free society, citizens should be left at least one unfettered means of communication which cannot be invaded without the showing of probable cause necessary for a search warrant. To allow the government to give an absolute monopoly and then to use it to invade the privacy of the citizenry without the protection of judicial scrutiny is to license the blatant circumvention of constitutional rights.[117]

This provides an extreme example of the more general argument against the presumption of voluntariness inherent in the third-party doctrine discussed *supra*.[118] As Judge Ferguson explains, the USPS provides a perfect illustration of an organization with which individuals must necessarily share limited information in order to engage in modern life. The USPS's governmental connections make both the lack of voluntariness and the potential for consequential corruption especially clear.

Even without the governmental piece, however, the Supreme Court has recently shown itself just as willing to limit the third-party doctrine on voluntariness grounds as on reasonability grounds. In the 2010 case *City of Ontario v. Quon*, the Court refused to conclusively determine whether a right to privacy existed for text messages stored on a workplace cell phone, noting that it would not "elaborat[e] too fully on the Fourth Amendment implications of emerging technology before

---

114. 532 U.S. 67, 70, 83–85 (2001); *see also* Henderson, *supra* note 12, at 439.

115. *See Ferguson*, 532 U.S. at 93–96 (Scalia, J., dissenting).

116. United States v. Miller, 425 U.S. 435, 443 (1976) (discussed *supra* note 85 and accompanying text); *see also* Henderson, *supra* note 12, at 440.

117. *Choate*, 422 F. Supp. at 270–71.

118. *See supra* pp. 1643–44, 1646 (detailing the general argument against voluntariness and quoting Justice Sotomayor's concerns regarding voluntariness in *Jones*).

its role in society has become clear."[119] It went on to clarify that "[c]ell phone and text message communications are [now] so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification," which may "strengthen the case for an expectation of privacy."[120] Again, this bolsters Judge Ferguson's conception of mail covers as outside normal third-party rules, and proves that his concerns with the third-party doctrine persist today.

At the appellate level in *Choate*, dissenting Judge Hufstedler also challenged the third-party doctrine on mail cover specific grounds, noting that the subject of a mail cover has neither control over which mail she receives nor any reason to suspect her mail is being recorded.[121] This compounds the voluntariness issue described above, because it makes the idea of a voluntary conveyance even less convincing for mail covers than for other forms of surveillance. When talking to an undercover informant, an individual is on notice that her words may be remembered and recounted.[122] When turning over checks or deposit stubs at a bank, an individual knows those documents need to be collected and the transactions they represent recorded so that the bank can maintain correct accounts.[123] When using a phone, an individual is aware the phone company keeps a record of calls made, and—at least at the time *Smith* was decided—saw that record each month in her phone bill.[124] And finally, when an individual drives on public streets, she is on notice that others are watching at least small portions of her journey.[125]

Yet, as Judge Hufstedler rightly acknowledges, this is not true in the case of mail covers: while an individual knows the Postal Service

---

119. 560 U.S. 746, 759 (2010).

120. *Id.* at 760.

121. United States v. Choate, 576 F.2d 165, 205 (9th Cir. 1978) (Hufstedler, J., dissenting):

> Mail covers differ [from other information, such as bank notes, that may be revealed to a third party] for a number of reasons. As noted above, the recipient of mail does not knowingly reveal anything [—] mail on its way to him is surreptitiously examined before it ever enters his possession. Moreover, the information in the form collected is not known by him to exist anywhere nor does he consent to its compilation. . . . [T]here is no reason for a mail cover suspect to assume that a list of all his correspondents has been compiled.

122. *See* United States v. White, 401 U.S. 745 (1971) (discussed *supra* note 84 and accompanying text).

123. *See* United States v. Miller, 425 U.S. 435 (1976) (discussed *supra* note 85 and accompanying text).

124. *See* Smith v. Maryland, 442 U.S. 735 (1979) (discussed *supra* notes 87–89 and accompanying text).

125. *See* United States v. Jones, 565 U.S. 400 (2012) (discussed *supra* Section II.A.2). It should be noted the driving individual, at least when not using GPS herself, is not aware others are *recording* any of her journey. In this regard, the GPS example is the closest case to mail covers.

must handle her mail in some minimal fashion, she does not know or expect that it will record even a single parcel, let alone all of her mailing transactions.[126] Thus, the idea of a voluntary conveyance of information *with knowledge that it may be recorded* that is arguably essential to the application of the third-party doctrine is not present in the case of mail covers. And again, because in the case of mail covers the government itself records the information, the situation is particularly problematic.

Similarly, in the context of mail covers, individuals have no choice over which parcels of mail they receive, unlike which individuals they choose to speak to, which banks they choose to transact with, which phone calls they choose to make and answer, and which roads they choose to drive on. Because it tracks mail the subject has not yet received and may never have asked for, the mail covers program also frequently collects information that is only precariously connected to its subjects. In addition, the program involves a concerning number of third-party rights by implicating the non-subject senders and receivers of the subject's mail.[127]

These issues—that mail covers are not reasonable, that the governmental and monopolistic nature of the USPS renders subjects' use of it involuntary, that subjects have no control over the mail they receive, and that subjects are unaware of even the possibility that their mail will be recorded—are unique to mail covers. Consequently, they make mail covers particularly concerning from a data-privacy perspective and serve to significantly undermine the third-party doctrine's application to mail cover surveillance. While the practical chance of any reversal of the mail cover program's constitutionality on these grounds is slim given the sheer number of years it has existed within the third-party landscape, then, this Note argues that, at least theoretically, mail covers are unconstitutional even under the third-party doctrine.

Alternatively, there is also an argument to be made that the third-party doctrine simply should not apply in the context of the mail covers program. This is because the Postal Service has been recognized in some case law as a bailee of mail parcels,[128] and there is evidence to

126. Of course, the government could make its mail recording procedures better known and (at least in a basic sense) solve this problem, but doing so would defeat the practical purpose of mail covers, which by nature require a kind of societal obliviousness.

127. *See, e.g.*, discussion *supra* note 68 and accompanying text (citing United States v. Choate, 576 F.2d 165, 188 (9th Cir. 1978) (Hufstedler, J., dissenting) and noting that "the rights of 'large numbers of citizens' beyond those whose mail is actually being tracked are implicated in mail cover investigations").

128. *See, e.g.*, U.S. Fid. & Guar. Co. v. United States, 246 F. 433, 435 (9th Cir. 1917) ("It is well settled that the United States is a bailee for hire of registered packages and their contents . . . ."); *see also* Lerakoli, Inc. v. Pan Am. World Airways, Inc., 783 F.2d 33 (2d Cir. 1986) (characterizing

suggest that "the third party doctrine [was never intended] to apply where the third party is a mere conduit or bailee."[129] Indeed, "[c]ourts in other contexts have recognized a reasonable expectation of privacy in something left with a bailee" that would overcome any third-party doctrine argument for mail cover constitutionality.[130] This would suggest that the very concept of mail delivery is privileged in some way that excludes it from the third-party doctrine's reach and requires extra care by the Postal Service sufficient to make warrantless searches of the parcels in their care unconstitutional.[131]

In a similar vein, the nature of the Postal Service's handling of mail calls into question the constitutionality of the mail covers program even under the property-based interpretation of the Fourth Amendment espoused by Justice Scalia in *Jones*. This is because, in order to record the relevant information, "government officials must take possession 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."[132] Admittedly, at first glance this does not seem nearly as significant as the trespass of officers attaching a tracking device to an individual's car in *Jones*. However, according to the legal definition of trespass, the brief taking of a mail parcel to record its outer contents remains an "unlawful act committed against the person or property of another,"[133] and an "act of direct physical interference with a chattel possessed by another."[134] Technically, then, it must be defined as a trespass, making the difference between a mail cover and the more egregious trespass described in *Jones* "one of degree, not quality."[135]

This argument would likely render all mail covers—or, at least, those implemented without the requisite standard of suspicion—

---

the USPS as a bailee of mail parcels, a characterization that was essential to the outcome of the case), *cert. denied*, 479 U.S. 827 (1986).

129. Henderson, *supra* note 12, at 438; *see also* Rawlings v. Kentucky, 448 U.S. 98, 104 (1980) (suggesting that an individual, in using a bailee to transfer or hold goods, takes a precaution to maintain her privacy, and therefore maintains a privacy interest over the goods). This approach implies that bailees are not to be treated as normal third parties, and thus that searches of property in the care of bailees are unreasonable, at least without the requisite standard of suspicion.

130. Henderson, *supra* note 12, at 437 n.36 (citing "United States v. Most, 876 F.2d 191, 198 (D.C. Cir. 1989) (bag left with store clerk); United States v. Barry, 853 F.2d 1479, 1481–84 (8th Cir. 1988) (luggage left with airline); United States v. Presler, 610 F.2d 1206, 1213–14 (4th Cir. 1979) (briefcase left with friend)").

131. Note that this concept could be applied to situations beyond mail—e.g., to email held by a service provider. *See id.* at 438 n.37.

132. Morrison, *supra* note 47, at 11.

133. *Trespass*, BLACK'S LAW DICTIONARY (10th ed. 2014).

134. *Trespass to Chattels*, BLACK'S LAW DICTIONARY (10th ed. 2014).

135. Morrison, *supra* note 45, at 11.

unconstitutional. Consequently, a property-based challenge of this sort would likely be unsuccessful. Theoretically considering such a challenge, however, illustrates once again the precariousness of the constitutionality of mail covers in particular as a mechanism of surveillance, under either the third-party doctrine or the property-based approach to the Fourth Amendment. It also serves to illuminate the new kinds of property-based legal challenges Justice Scalia's opinion in *Jones* may foster in privacy law generally.[136]

2. The Mosaic Theory, Revisited

The potential adoption of the mosaic theory offers particularly fruitful avenues of challenge to the mail covers program. As Steven Morrison has argued on behalf of the National Association of Criminal Defense Lawyers,

> [T]he 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.[137]

Judge Hufstedler made this point in his dissent in *Choate*, noting that mail covers can be viewed as even more invasive than "surveillance of [an individual's] movements."[138] This is because mail covers provide access to information many individuals seek to keep private, such as their political and religious affiliations, domestic and foreign contacts, online purchases, and other information that could not necessarily be gleaned even from the extensive GPS surveillance disallowed in *Jones*.[139]

Additionally, mail covers already extend the basic period of surveillance two days beyond that rejected for GPS surveillance in *Jones*,[140] and the history of the mail covers program reveals that even

---

136. Scholars since *Jones* have suggested, for example, that the government's interception of phone and email communications constitute electronic trespasses. *See, e.g.*, Erica Goldberg, Commentary, *How* United States v. Jones *Can Restore Our Faith in the Fourth Amendment*, 110 MICH. L. REV. FIRST IMPRESSIONS 62, 68 (2011) ("Even in the *Katz* electronic surveillance case, the Court could have retained the connection between property rights and privacy rights by holding that an electronic connection to an individual's property (or to the phone company's property) is a physical intrusion, albeit on a microscopic level."); *see also* Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 12–13 (2012) (describing the attempts of scholars to rejuvenate property-based Fourth Amendment challenges in the wake of *Jones*).

137. Morrison, *supra* note 45, at 11.

138. United States v. Choate, 576 F.2d 165, 203 (9th Cir. 1978) (Hufstedler, J., dissenting).

139. United States v. Jones, 565 U.S. 400 (2012); *Choate*, 576 F.2d at 202 (Hufstedler, J., dissenting); *see also supra* pp. 1637–38 (discussing amount of information mail covers can collect).

140. Mail covers are initially implemented for thirty days, where the GPS surveillance in *Jones* was for twenty-eight days. *See Jones*, 565 U.S. at 403; *Choate*, 576 F.2d at 187 n.11.

that duration is often extended further, to 120 days or more, with little oversight.[141] Compounding this problem, less scrutiny is initially needed to implement mail covers than other forms of surveillance. This is particularly true given that the "reasonable grounds" required to begin a mail cover do not even need to be true according to the majority in *Choate*, a reading in line with current mail cover regulations.[142] Mail covers are also particularly cheap for the government to implement compared to other surveillance techniques. The secretive Mail Imaging and Mail Isolation Control and Tracking programs introduced in the early 1990s and 2000s[143] only increase these worries, and look even more like the kind of "dragnet type law enforcement practices"[144] the Court's decision in *Jones* is meant to protect against. All of this suggests both that mail covers are uniquely designed to create a mosaic-style picture of an individual's life and that they are particularly vulnerable to abuse. Both of these conclusions make mail covers unusually viable candidates for unconstitutionality under the mosaic theory.

Indeed, in her dissenting opinion in *Choate*, Judge Hufstedler actually sought to apply an early version of the mosaic theory, noting:

> While an individual may realize that an isolated piece of mail may attract the attention of postal employees, he knows that ordinarily no one would have the ability or inclination to remember who writes to him. . . . Thus, while we might concede that a sender or recipient of mail impliedly consents to the visual inspection of the exterior of any individual piece of mail for a purpose connected with postal service, he cannot be said to thereby acquiesce in the storage of the information which creates a "data bank" usable against him which would not otherwise exist. [This is particularly true because] the compilation of data [regarding the subject's relationship with both individuals and organizations] obtained through a mail cover exposes the personal life of the subject before law enforcement agencies in a manner unobtainable even through surveillance of his movements.[145]

---

141. *See supra* note 70 and accompanying text.

142. *Choate*, 576 F.2d at 172 ("The regulations simply do not require the specification of the factual predicate upon which the requesting agency bas[e]s its conclusion that the mail cover subject is involved in the commission or attempted commission of a crime. Failure to specify this predicate is proper under the regulations.").

143. *See* discussion *supra* Section I.B.

144. United States v. Knotts, 460 U.S. 276, 284 (1983). *Knotts* applied the third-party doctrine to find the government's use of a beeper to track the location of an individual's car for three days constitutional. *Id.* at 285. In *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), the D.C. Circuit Court's decision preceding *Jones*, 565 U.S. at 400 (both discussed *supra* Section II.B), the D.C. Circuit quoted dicta from *Knotts* stating that "dragnet-type law enforcement practices," such as twenty-four-hour surveillance of an individual, may involve "different constitutional principles" than those considered in the third-party doctrine. *Maynard*, 615 F.3d at 556 (quoting *Knotts*, 460 U.S. at 283–84). The D.C. Circuit relied on this dictum to distinguish the long-term GPS surveillance involved in *Maynard* and *Jones* from the limited beeper surveillance involved in *Knotts*. *Id.* The court then took the opportunity to introduce the mosaic theory as a valid alternative to the third-party doctrine where long-term surveillance is at issue. *Id.*

145. *Choate*, 576 F.2d. at 202–03 (Hufstedler, J., dissenting). Note that Justice Hufstedler also had concerns that this kind of broad, all-inclusive mail cover posed significant First Amendment

In other words, Judge Hufstedler made the mosaic-style argument that, although the information collected by mail covers is noncontent-based metadata, it can be excessively revealing when enough is collected and considered together. This realization led to her assertion that mail covers violate a subject's reasonable expectation of privacy.[146] Significantly, this proves that even as far back as 1978—over thirty years before the *Jones* decision—some judges disagreed with a stringent, blanket application of the third-party doctrine to surveillance cases, and opted instead to apply a version of the mosaic theory when cases involved broad-based surveillance techniques. It also reveals that, on the only occasion a judge considered a mail cover in the context of the mosaic theory, she found it unconstitutional.

To summarize, then, under any theory of Fourth Amendment law—be it the mosaic theory, the third-party doctrine, or even the pre-*Katz* property-based approach—the constitutionality of mail covers under the Fourth Amendment is precarious at best. As a result, the next Part will consider how the courts could, if given the opportunity, use one of the legal challenges outlined above to encourage substantial reform of both the mail covers program specifically and surveillance initiatives generally.

III. THE ELEMENTS OF LASTING REFORM

A ruling of unconstitutionality for an individual mail cover would likely be insufficient to fix the longstanding history of abuse of the mail covers program or serve to ensure such abuse did not continue. However, such a ruling would indicate that the Court is serious about privacy protections in an age of technological advancement. It would also spur renewed congressional debate about the mail covers program—debate that has stalled in recent years as attention has shifted to more egregious abuses of newer surveillance initiatives.[147] Indeed, this congressional apathy, coupled with the historical ineffectiveness of congressional reform of the program without heightened enforcement power, is exactly why it is so essential that the Court finally take up a mail covers case. Addressing the corruption of surveillance power through the lens of a surveillance technique as well-

issues. *See id.* However, because mail covers and mail issues generally have been treated squarely as Fourth Amendment issues since the earliest mail communications case, *Ex parte Jackson*, 96 U.S. 727 (1877), this Note does not address the First Amendment question.

146. *Choate*, 576 F.2d. at 202–03 (Hufstedler, J., dissenting).

147. *See, e.g.*, *supra* note 63 (noting that the nearly exponential growth of the mail covers program in recent years coupled with an absence of new regulations or even congressional discussion regarding the program suggests apathy towards it).

established as the mail covers program—a program that in many ways laid the groundwork for the creation and expansion of surveillance initiatives generally—would send a clear signal that the Fourth Amendment is not a dead letter when it comes to privacy protections.

Should such a case be brought, or should Congress choose to address the program through legislation, there are a number of opportunities for reform that would force the government to conduct mail covers in a manner more protective of privacy rights and more in line with the Fourth Amendment. There are also a number of opportunities for reform that would allow the judicial system to better prevent abuses of government surveillance power generally. This Part considers some of those opportunities for reform. Section A addresses the reforms capable of improving the mail covers program specifically, and Section B addresses the doctrinal reforms capable of improving judicial analysis of surveillance cases generally.

A. Mail Cover Reforms

A number of reforms could serve to improve the mail covers program. First, a better system of enforcement should be established to ensure that even the minimal standards of 39 C.F.R. § 233.3 are followed. Implementing a quasi-judicial system to ensure that mail covers are only granted where appropriate and for as long as necessary would address this issue. At a minimum, heightened oversight protocols within the USPS are needed to address the problems of inadequate justification for and automatic renewal of mail covers detailed *supra*.[148] Additionally, Congress needs to ensure that any remaining instances of negligence or abuse in the implementation of mail covers do not inadvertently benefit government prosecutions. This could be achieved via the passage of "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 [39 C.F.R § 233.3]."[149] Such action would address a major issue in *Choate*, for example, wherein the data gleaned from the mail cover were accepted despite evidence that the requesting agent had falsified statements in order to implement the cover.[150] Another, more explicit, method of dealing with the falsification

148. Morrison, *supra* note 47, at 20; *supra* Section I.B.

149. Morrison, *supra* note 47, at 20.

150. *Choate*, 576 F.2d at 194 (Hufstedler, J., dissenting) (noting that evidence had established that the requesting officer did not have any information supporting his accusations that defendant Choate was involved in a smuggling operation, that defendant Choate was in contact with a South American smuggler, or that the mail cover would assist in any investigation other than the IRS investigation opened after the mail cover had already been implemented).

issue is for Congress to amend § 233.3 to require that the "reasonable grounds" needed to request a mail cover are based on reliable evidence.[151]

Second, the data collected via mail covers should be retained for less than the current eight years. It is true that this eight-year requirement was implemented to encourage transparency and help defendants, some of whom were being indicted significantly after their mail cover had been issued, and who therefore could not access mail cover records that had already been destroyed.[152] However, eight years is an excessive period of time to retain such extensive data. National security-related telephony metadata is currently retained for only five years, and there is no justifiable reason to suggest that mail covers should be stored longer.[153] Congress should determine a nonarbitrary amount of storage time for mail cover data that will best serve the interests of both government agencies and potential defendants without retaining the data for longer than is strictly necessary.

Finally, far more transparency should be required regarding the new mail imaging systems that photograph and record, for unknown purposes and lengths of time, the outside of every parcel of mail delivered by the USPS. A congressional report on these programs would clarify why they are necessary and what benefits they serve. These programs represent the exact kinds of indiscriminate, dragnet surveillance systems that the Court has frequently been concerned with, and the public should have access to more information about their use. This is particularly true given that almost all citizens use the USPS in some capacity and are consequently affected by the systems.

B. Doctrinal Reforms

A number of reforms could also serve to improve judicial analysis of surveillance cases generally. First, the Court should explicitly reject the third-party doctrine and embrace the mosaic theory. The third-party doctrine's presumption of voluntariness in an individual's

151. In *Choate*, the agent requesting the mail cover noted: "It is felt that CHOATE and the source in South America correspond by mail." United States v. Choate, 422 F. Supp. 261, 265 (C.D. Cal. 1976). Judge Ferguson was adamant in his district court opinion that "an agency's mere 'feeling' that criminal activity is afoot [should not be] sufficient to provide the needed showing [of 'reasonable grounds']." *Id.* at 266.

152. *See, e.g.*, *Choate*, 576 F.2d at 209 (Hufstedler, J., dissenting) ("[U]nder the old, two-year cycle, Choate would have found that all records of the mail cover request had been destroyed prior to his indictment over two years later; undoubtedly other criminal defendants may find records have been destroyed when pre-indictment investigation exceeds eight years.").

153. *See* Morrison, *supra* note 47, at 23 ("[I]f national security-related telephony metadata is retained only for five years, the retention of more mundane mail cover data for eight years seems arbitrary.").

conveyance of personal data has always been a legal fiction. The mail covers program, effective in tracking such data for so long only because of the government's convenient monopoly over mailing, presents a particularly clear example of this.[154] The mosaic theory's contextual framework provides a more common sense approach to *Katz*'s original "reasonable expectation of privacy" test.

Critics who argue that such a drastic change would be too disruptive to the legal system[155] forget, first of all, that the underpinnings of the mosaic theory have been around for decades. The idea that the excessive collection of data should be unconstitutional even where individual instances of the same kind of collection are constitutional has long existed as a counterpoint to the third-party doctrine. The mosaic theory itself was first introduced in Freedom of Information Act cases in 1972,[156] and Judge Hufstedler's dissent in *Choate* reveals that judges have been willing to implement some form of it in surveillance cases since at least 1978.[157]

Critics also forget that there are many iterations a fully formed mosaic theory could take, not all of which need be excessively disruptive. For example, the Court could implement a kind of threshold test for mosaic theory applicability. This would allow the Court to use the traditional "sequential approach" to analyzing a search or seizure—whereby individual searches or seizures are examined in isolation[158]—unless the type of search or seizure in question involved the use of a surveillance mechanism designed to indiscriminately collect as much information about an individual as possible, thereby forming a mosaic picture of her life.[159] A court could then ask, if the mosaic theory applied, whether the surveillance mechanism had been used in such an indiscriminate and invasive manner as to be unreasonable.[160] This

154. *See supra* note 117 and accompanying text (quoting district court Judge Ferguson in *Choate*).

155. *See, e.g.*, Kerr, *supra* note 110, at 352–53.

156. Smith Dennis, *supra* note 13, at 744 n.42.

157. *See supra* notes 145–146 and accompanying text.

158. *See* Kerr, *supra* note 110, at 315 ("Fourth Amendment analysis traditionally has followed what I call the sequential approach: to analyze whether government action constitutes a Fourth Amendment search or seizure, courts take a snapshot of the act and assess it in isolation.").

159. This idea of analyzing searches or seizures differently based on their relative invasiveness is analogous to an approach to Fourth Amendment jurisprudence espoused by Professor Christopher Slobogin and known as the "proportionality principle." This principle "requires that the justification for a search be roughly proportional to its intrusiveness." Slobogin, *supra* note 136, at 14.

160. As noted by Kerr, judges at this point differ on what "unreasonable" means in relation to a mosaic theory: Justice Alito focused on surveillance beyond what a reasonable citizen would expect; Justice Sotomayor focused on surveillance that allowed the government to obtain information about specific citizens "more or less at will"; and Justice Ginsburg of the D.C. Circuit in *Maynard* focused on the "likelihood that private actors would conduct similar surveillance."

would allow a majority of search and seizure cases to remain unaffected by the adoption of mosaic theory in surveillance scenarios. It may also encourage law enforcement to use broad-based surveillance techniques in more specific ways—for example, by targeting specific locations or mailing addresses rather than collecting cumulative data about all the places an individual goes or all the mail she sends and receives.

It is true, in other words, that the adoption of the mosaic theory would "open a wide range of new questions for the court to answer," including when and how the theory should be applied.[161] This should be seen, however, as an opportunity to make the Fourth Amendment work again in an age of unprecedented surveillance capability that is simply incompatible with a stringent third-party doctrine. If nothing else, the history of the mail covers program proves that broad-based surveillance initiatives are consistently abused despite congressional attempts at reform.[162] A Fourth Amendment doctrine with more enforcement "bite" is therefore essential to curbing surveillance corruption.

Even with a mosaic theory framework in place, however, other doctrinal changes are necessary to ensure that courts are able to hold surveillance programs accountable. Chief among these are changes to current standing and discovery laws. Present standing laws preclude individuals from bringing a case unless they can prove an "injury in fact," meaning they can at least show that some concrete harm has been caused or will be imminently caused by a defendant's actions.[163] Given that surveillance initiatives are by necessity highly secretive, plaintiffs are rarely able to meet this high standard, leaving most surveillance cases to be dismissed for lack of standing.[164] The fact that only a handful of mail cover cases have been litigated despite the mail covers program being more than a century old makes this fact painfully clear. In order to ensure that judicial enforcement of surveillance programs is a real

---

United States v. Jones, 565 U.S. 400, 417–430 (2012); United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010); Kerr, *supra* note 110, at 330–31. These ambiguities would need to be addressed, but the Court is well equipped to determine a new reasonableness standard of this sort.

161. Kerr, *supra* note 110, at 329.

162. *See* discussion *supra* Part I. Such consistent abuse in spite of congressional attention can be found in nearly every other surveillance program of which the public is aware, as evidenced by Edward Snowden's revelations, discussed *supra* in the Introduction. It is for this reason that statutory reform alone will not be sufficient to address surveillance abuses.

163. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (applying this high standing standard to cases involving surveillance initiatives).

164. *See* Christopher Slobogin, *Standing and Covert Surveillance*, 24 PEPP. L. REV. 517, 518, 522 (2015) (noting that *Clapper*'s high standard combined with the covert nature of modern surveillance initiatives makes it nearly impossible for plaintiffs to get standing in surveillance cases); *see also* Marguerite Rigoglioso, *Civil Liberties and Law in the Era of Surveillance*, STAN. LAW., Fall 2014, https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance/ [https://perma.cc/2LQS-MUTE]; Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 ISJLP 551, 552 (2014).

threat, and thus that surveillance officers know they may be prosecuted for missteps, these standing rules must be changed.

These standing reforms could be implemented via the Court overruling its prior precedent on the matter or via Congress taking action to lower the requisite standing for secret surveillance cases. The Court or Congress could, for example, "authorize challenges to programs so long as plaintiffs could show there was a 'reasonable likelihood' that their communications would be intercepted by the government," rather than requiring "certainty" of impending interception.[165] Alternatively, Congress could require more internal oversight for secret surveillance programs, for example by requiring greater adversarial processes in the Foreign Intelligence Surveillance Court.[166] Both options would allow more surveillance cases to be tried before a judicial body, bolstering enforcement mechanisms and, hopefully, ensuring better surveillance practices.

It should be acknowledged that such reform would constitute a major change to longstanding judicial practice regarding standing. However, standing requirements were originally implemented to prevent frivolous lawsuits and maintain appropriate separation of powers within the different branches of government.[167] Expanding standing specifically for surveillance cases upsets neither of these goals.[168] In fact, because unregulated surveillance chills the ability of individuals to live in full intellectual freedom, and thus "undermines interests 'essential to political participation,' " such an expansion in standing laws is crucial to ensure the viability of democracy itself.[169]

In order for changes in standing standards to have any meaning, though, some greater compliance with discovery laws also needs to be enforced to ensure plaintiffs have access to relevant information. The *Choate* mail cover case provides an excellent example of why this is necessary. There, the defendant, despite multiple discovery requests and a requirement in 39 C.F.R. § 233.3 that any information relating to a mail cover be revealed through appropriate discovery procedures, only discovered he had been the subject of a mail cover inadvertently, through an attorney's misstep during an unrelated hearing.[170] Unless

---

165. Vladeck, *supra* note 164, at 555.

166. *Id.* Note that Slobogin has questioned whether such internal oversight would really be effective in garnering any change in surveillance practice. *See* Slobogin, *supra* note 164, at 529.

167. *See* Slobogin, *supra* note 164, at 531.

168. *See id.* at 532–33.

169. *Id.* at 538 (quoting JOHN HART ELY, DEMOCRACY AND DISTRUST 136 (1980)). For an excellent analysis of this concept as addressed in the political process theory of constitutional interpretation, see *id.* at 538–41.

170. The tendency for the government to ignore discovery requests for surveillance data, even when statutorily obligated to provide such data upon request, is not limited to the context of mail

law enforcement agencies are honest in discovery procedures and provide the secret surveillance information required of them, plaintiffs have no hope of finding essential evidence on their own.

Greater punishments for data suppression could help solve this problem, and should be implemented. In conjunction, courts could require proof that secret surveillance did not occur in cases where a plaintiff can provide reliable evidence that it likely did. For example, where a plaintiff reasonably makes a discovery request for surveillance records and the government asserts that those records do not exist, the court could require a sworn statement to that effect from the officers in charge of the surveillance initiative in question. This would at least create a stronger system of accountability amongst surveillance officers.

Finally, it is essential that the Court reinvigorate the distinction between criminal law cases and national security cases in order to ensure that broad conceptions of national security are not being used to inappropriately justify overbroad surveillance procedures on suspects accused of standard criminal activity.[171] The history of mail covers—wherein a specific definition of national security had to be implemented within § 233.3 to prevent its overuse as a justification—exemplifies this point as well.[172] National security cannot be a blanket justification for surveillance if the protection of privacy rights is to be taken seriously.

Each of these reforms would serve to better protect the privacy of individuals without drastically altering the surveillance landscape or hindering investigatory operations. Together, they could help increase accountability and transparency, decrease corruption, and allow the judicial system to act as a true check on government surveillance capabilities. In order to foster greater public trust of government programs, they should be implemented.

CONCLUSION

This Note has outlined the history of mail covers, examined the relevant evolution of Fourth Amendment law and the potential fate of

covers. Slobogin has noted that the Department of Justice has regularly ignored the notice and disclosure requirements of the Foreign Intelligence Surveillance Act. *Id.* at 523. Other government agencies frequently find loopholes to avoid these requirements altogether. *Id.* Additionally, many other surveillance-related statutes, such as those governing the "metadata and PRISM programs that collect phone and Internet information," do not have any notice or disclosure requirements and may, in fact, forbid notice or disclosure. *Id.* at 524. The point is simply that a lack of notice and disclosure in discovery is a systemic problem in surveillance cases that needs to be addressed if plaintiffs are to have any hope of succeeding in litigation.

171. *See* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE 150–58 (2016).

172. *See* discussion *supra* note 38 and accompanying text.

the mail covers program in light of that evolution, and offered reforms that could improve the mail covers program and Fourth Amendment jurisprudence moving forward. It may seem strange, to some, to take the time to consider privacy and surveillance law through the framework of a program so technologically outdated as the mail covers program, but such thinking is in error. The mail covers program laid the groundwork for nearly every modern surveillance initiative, and apathy towards the abuse inherent in that program in many ways led to the apathy surrounding surveillance today. The history of the mail covers program, in short, reveals that a change to our collective attitude towards surveillance and our enforcement of surveillance initiatives has been needed for decades, if not centuries. It also reveals that such a change is possible, and need not disrupt essential foundations of Fourth Amendment jurisprudence.

Many today also argue that a lack of privacy is a small price to pay for increased security in an age of terror. Such critics would question the validity of any discussion critiquing security-related surveillance initiatives, including this one. But this thinking, too, is in error. The right to privacy forms the very foundation of freedom. Where privacy is lost, freedom of speech and association are in jeopardy, and democracy in peril. History, ravaged as it is with totalitarianism, fascism, and resultant oppression, proves this point all too well. Indeed, the Fourth Amendment was itself enacted to protect American citizens from the tyranny of general warrants that allowed British officers to search any home they desired and quell any indication of revolution they found.[173] The point is simply that privacy is not the opposite of security; rather, it is the prerequisite.

*Julie Lynn Rooney**

173. *See, e.g.*, Payton v. New York, 445 U.S. 573, 583 (1980) (describing the origins of the Fourth Amendment).

* J.D. Candidate, 2018, Vanderbilt University Law School; B.A., 2015, Denison University. To my parents, Tim and Janet Rooney, for their love; to my siblings, Kathleen and Patrick Rooney, for their influence; to my Professors, particularly Christopher Slobogin, for their wisdom; to my friends, too many in number to name, for their encouragement; to the editors and staff of the *Vanderbilt Law Review*, for their insight; to the members of the legal community fighting to protect privacy rights, for their dedication: words are not enough, but they are what we have. So I say: thank you.