20-1653(L)

20-3945(CON)

United States Court of Appeals

for the

Second Circuit

MICROSOFT CORPORATION,

Appellant,

– v. –

UNITED STATES OF AMERICA,

Appellee.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK (BROOKLYN)

BRIEF FOR FORMER FEDERAL PROSECUTORS *AMICI CURIAE* IN SUPPORT OF APPELLANT

Krieger Kim & Lewin LLP
Edward Y. Kim
500 Fifth Avenue
New York, New York 10110
Telephone: (212) 390-9550

Cleary Gottlieb Steen & Hamilton LLP
Jonathan S. Kolodner
Rahul Mukhi
Benjamin D. Bright
One Liberty Plaza
New York, New York 10006
Telephone: (212) 225-2000
Attorneys for Amici Curiae

December 21, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

STATEMENT OF INTEREST OF *AMICI CURIAE*

Amici Curiae Former Federal Prosecutors respectfully submit this brief, pursuant to Rule 29 of the Federal Rules of Appellate Procedure, in support of appellant.[1] A list of the *amici curiae* is provided in the Appendix.

Amici are former prosecutors in the Southern and Eastern Districts of New York and current white-collar defense attorneys whose law enforcement experience includes pursuing sensitive investigations of large companies. *Amici* have a unique perspective on achieving a balance between preserving the integrity of ongoing investigations while also protecting constitutional rights. Accordingly, *amici* write to assist the Court in understanding how law enforcement can operate effectively while allowing cloud-services providers such as Microsoft to exercise their First Amendment rights to provide appropriate notice to their customers when the government is seeking those customers' data.

Amici recognize that certain exceptional circumstances—such as witness safety or operational integrity—may justify the issuance of a secrecy order under the Stored Communications Act ("SCA"), 18 U.S.C. § 2705(b). At the same time,

---

[1] The parties to this appeal consent to the filing of this brief. No counsel for any party authored this brief in whole or in part. No person or entity other than *amici curiae* and their counsel contributed money to fund the preparation or submission of this brief. The views of *amici* expressed in this brief do not necessarily reflect the views of the firms, companies, or institutions with which they are or have been affiliated.

amici believe that new technologies should not be exempt from traditional constitutional safeguards: the issuance of a § 2705(b) secrecy order must be justified by a specific and meaningful showing and must be narrowly tailored to promote a compelling government interest and be the least restrictive means of achieving that interest.

As explained below, *amici*'s experience as former federal prosecutors shows that § 2705(b) secrecy orders with *no* exceptions for *multiple years*—such as the one at issue in this case—are ordinarily unnecessary in connection with corporate investigations. This is particularly true when the target company is a large, public company, given that such entities often have sophisticated in-house counsel and compliance personnel with experience dealing with sensitive government investigations. While *amici* are not privy to all information available to the parties, based on the public record we have reviewed, *amici* respectfully submit that the District Court did not properly hold the government to its burden to show that the secrecy order here is narrowly tailored to promote a compelling government interest and is the least restrictive means of achieving that interest—especially in light of Microsoft's proposed less restrictive alternative.

BACKGROUND

Section 2703 of the SCA authorizes the government to compel an "electronic communication service or remote computing service," which has been interpreted to include cloud-services providers such as Microsoft, to provide the contents of electronic communications pursuant to a warrant without the government providing notice to the person or enterprise customer whose communications are being searched or seized. 18 U.S.C. § 2703(b). Section 2705(b) in turn authorizes the government acting pursuant to § 2703 to seek an order from a court compelling service providers "not to notify any other person of the existence of the warrant, subpoena, or court order." 18 U.S.C. § 2705(b). These "[j]udicial gag orders impinge upon freedom of speech and press under the First Amendment, and must pass muster under well-established constitutional case law." *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 880 (S.D. Tex. 2008); *see Gannet Co., Inc. v. DePasquale*, 443 U.S. 368, 399 (1979) (Powell, J., concurring) (describing "gag order[s]" as "one of the most extraordinary remedies known to our jurisprudence" (internal quotation marks omitted)).

In light of this, SCA secrecy orders must satisfy strict scrutiny: the government must show that it has a compelling government interest in the speech restriction, that there is no less restrictive alternative to protect that interest, and

that the speech restriction is narrowly tailored to the compelling government interest. *See Matter of Subpoena 2018R00776*, 947 F.3d 148, 155–56 (3d Cir. 2020). Section 2705(b) provides a list of government interests that could potentially justify a secrecy order, including, as relied upon by the government here, that notification will result in "seriously jeopardizing an investigation." 18 U.S.C. § 2705(b)(5).

Amici do not dispute that certain circumstances may justify the issuance of a secrecy order to achieve these legitimate government interests, including to protect an ongoing government investigation, but such circumstances are and should be rare. "The security of one's privacy against arbitrary intrusion by the police . . . is basic to a free society." *Wolf v. Colorado*, 338 U.S. 25, 27 (1949). Prosecutors are entrusted with safeguarding that right.

Federal courts have long sought to balance individual liberty and public safety as new technologies emerge, and they have recognized the particular constitutional hazards presented by police surveillance and secret warrants that fail to provide notice to the person who is surveilled or whose property is searched or seized. And law enforcement officials have long carried out investigations effectively under these constitutional safeguards—and can continue to do so, even with technological developments.

Accordingly, when determining whether the government has met its demanding burden under the strict scrutiny analysis—and particularly whether the government has shown a compelling interest in protecting its investigation that cannot be achieved here by a less restrictive alternative—we respectfully urge the Court to consider that, in the experience of *amici*, in the great majority of cases, the government need not employ measures such as a secrecy order with no exceptions to successfully pursue a corporate criminal investigation.

ARGUMENT

I. Notice to the target of a government search serves an essential constitutional function and may be delayed only in strictly limited circumstances.

In evaluating whether the government has shown that the secrecy order is narrowly tailored to a compelling interest in preserving the integrity of its investigation, the Court should consider the very limited circumstances under which courts have determined that searches or seizures conducted without notice to the targets are justified and necessary. These circumstances are appropriately limited because courts recognize the crucial role of such notice in upholding key constitutional protections.

"A conventional warrant ordinarily serves to notify the suspect of an intended search." *Katz v. United States*, 389 U.S. 347, 355 n.16 (1967). Without such notice, the warrant cannot serve one of its essential functions, which is to

"assure[ ] the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search." *United States v. Chadwick*, 433 U.S. 1, 9 (1977), *abrogated on other grounds by California v. Acevedo*, 500 U.S. 565 (1991). Those individuals deprived of notice are unable to bring lawsuits that challenge the legality of the warrant because they have no awareness of its existence.[2]

For this reason, SCA warrants accompanied by a § 2705(b) secrecy order prevent ordinary judicial processes from serving as a check on executive power: "excessive secrecy effectively shields electronic surveillance orders from appellate review, thereby depriving the judiciary of its normal role in shaping, adapting, and updating legislation to fit changing factual (and technological) settings over time." Stephen Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L & POL'Y REV. 313, 326 (2012). Without this judicial check, the "careful balance between privacy and security set by Congress is inevitably washed away by a torrent of secret orders, unrestrained by the usual adversarial and appellate processes." *Id.* at 331.

---

[2] As explained in further detail below, *see* infra pp. 9–11, the Second Circuit does recognize limited exceptions to providing notice to the targets of government searches. For example, in the context of covert-entry searches for intangibles, the Second Circuit has held that notice to the target may be delayed for a reasonable period of time not to exceed seven days upon "a showing of reasonable necessity for the delay." *United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990); *accord United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986).

The Supreme Court has recognized that if Fourth Amendment jurisprudence fails to keep pace with new technologies deployed by law enforcement, citizens would be left "at the mercy of advancing technology." *Kyllo v. United States*, 533 U.S. 27, 35 (2001); *see also United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010) ("[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."). Section 2705(b) secrecy orders thereby implicate not only Microsoft's First Amendment free speech rights, but also the development of sound Fourth Amendment case law because targets of government searches are prevented from bringing suits that challenge the legality of § 2703 warrants. In *amici*'s experience, not only law enforcement officials and targets but, indeed, the whole criminal justice system benefit from such judicial oversight.

Covert searches are not, of course, *per se* unconstitutional, *Dalia v. United States*, 441 U.S. 238, 247 (1979), and *amici* recognize the importance of allowing law enforcement officers to execute covert searches in certain circumstances pursuant to a warrant. But because their secrecy raises weighty constitutional concerns, Congress and the federal courts long ago established strict limitations on covert searches and require notice to the target of the warrant after a reasonable time. Law enforcement officials have operated effectively under these

constitutional safeguards for decades. The advent of new technologies, such as cloud computing, does not prevent them from continuing to do so.

a. Electronic surveillance.

In the Supreme Court's wiretap jurisprudence, the twin requirements that the government make a showing of particularized facts justifying the intercept and eventually provide notice to the targets are crucial to upholding an electronic surveillance law's constitutionality. In *Berger v. New York*, 388 U.S. 41 (1967), the Supreme Court held a New York wiretapping statute unconstitutional because it had "no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts." *Id.* at 60. A "showing of exigency, in order to avoid notice would appear more important in eavesdropping, with its inherent dangers, than that required when conventional procedures of search and seizure are utilized." *Id.*

The Supreme Court upheld, by contrast, the federal wiretapping statute that "provided a constitutionally adequate substitute for advance notice by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance." *Dalia*, 441 U.S. at 248 (citing *United States v. Donovan*, 429 U.S. 413, 429 n.19 (1977)). For the same reason, the Court upheld the constitutionality of covert entries to install electronic bugging equipment, recognizing that the statute's "detailed restrictions . . .

guarantee that wiretapping or bugging occurs only when there is a genuine need for it and only to the extent that it is needed." *Id.* at 250. These detailed restrictions include requiring (among other things) that the government provide a detailed description of the facts and circumstances that justify the electronic intercept, a full and complete statement as to whether other investigative procedures have been tried and failed or why they reasonably appear likely to fail or too dangerous, and a statement of the period of time the electronic intercept will be maintained. 18 U.S.C. § 2518(1). The statute also requires that notice of the electronic intercept be provided "[w]ithin a reasonable time *but not later than 90 days*," both to the target and to "other parties to intercepted communications as the judge may determine . . . is in the interest of justice." 18 U.S.C. § 2518(8)(d) (emphasis added).

b. Delayed notice warrants.

Federal courts have also upheld the constitutionality of delayed notice warrants, also known as "sneak-and-peak" warrants, which allow law enforcement to enter private premises, make observations, and leave without disturbing the contents or providing notice to the person whose property was searched. The

purpose of such delayed notice warrants is "to permit an investigation without tipping off the suspect." *United States v. Mikos*, 539 F.3d 706, 709 (7th Cir. 2008).

In 1990, the Second Circuit established two constitutional safeguards for delayed notice warrants in order "to minimize the possibility that the officers will exceed the bounds of propriety without detection." *Villegas*, 899 F.2d at 1336. First, law enforcement officers must make "a showing of reasonable necessity for the delay" and must demonstrate "good reason." *Id.* at 1337. Second, to authorize the delayed notice, a court must "require the officers to give the appropriate person notice of the search within a reasonable time after the covert entry." *Id.* While what constitutes a reasonable time may depend on the circumstances, the issuing court may not authorize a delay of more than *seven* days. *Id.* The warrant applicant is authorized to seek an extension, but each time must "make a fresh showing of the need for further delay." *Id.* (citing *Berger*, 388 U.S. at 59–60). The Second Circuit concluded that "[i]f these limitations on the withholding of notice are followed . . . the interests of both the individual and the government will be adequately served." *Id.* at 1337–38.

In 2001, Congress codified delayed notice warrants in 18 U.S.C. § 3103a. Pursuant to the statute, the government is required to make a showing of "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result." 18 U.S.C. § 3103a(b)(1).

Furthermore, the government must notify the target of the search "within a reasonable period not to exceed 30 days after the date of its execution." 18 U.S.C. § 3103a(b)(3). Similar to the safeguards established in *Villegas*, the statute authorizes extensions of this delayed notice, but these extensions may "only be granted upon an updated showing of the need for further delay" and "each additional delay should be limited to periods of 90 days or less." 18 U.S.C. § 3103a(c).

II. Law enforcement officials have effectively operated under constitutional safeguards that require particularized showings and eventual notice to search targets, and can continue to do so in the cloud.

An examination of these statutes, each of which balances important law enforcement interests against constitutional protections, shows that law enforcement officials have for decades conducted effective investigations under robust constitutional safeguards that reasonably prompt eventual notice to targets of searches or seizures. Accordingly, the government must be held to its burden to show adequate justification for the secrecy order here—which was issued after approximately two prior years of non-disclosure—beyond the mere existence of a routine corporate law enforcement investigation.

Congress enacted the federal wiretapping statute in 1968, so for more than 50 years law enforcement officials have utilized wiretaps with the understanding that they would be required to disclose to the search target the existence of the

wiretap within 90 days. Likewise, as noted above, beginning 30 years ago, law enforcement officials operating within the Second Circuit's jurisdiction have executed delayed notice warrants with the understanding that they would have seven days to disclose to the target that they had performed a covert search of his or her property. The government could seek an extension of the delayed notice, but only upon a "fresh" showing of necessity. *Villegas*, 899 F.2d at 1337. Over the last several decades, this limited delay of notice to search targets has become a routine part of the work of law enforcement. When Congress codified delayed notice warrants in 2001, it retained the requirement that notice be provided to the target of the search, albeit increasing the period of time the government has to provide such notice from seven to 30 days.[3]

In contrast to these statutory notice schemes, the government is not required to provide any notice to the subscriber or customer pursuant to a 2703(b) warrant. *See* 18 U.S.C. § 2703(b)(1)(A). Given that the government further seeks to restrain

[3] Empirical data regarding delayed notice warrants shows that notice requirements do not prevent law enforcement from employing these warrants in aid of investigations with regularity. Indeed, the Delayed-Notice Search Warrant Report for 2019 indicates that a total of 18,106 delayed warrant requests were reported that year in 92 federal judicial districts, of which 18,067 were granted; and 11,923 delayed warrant extension requests were reported that year, of which 11,885 were granted. *Delayed-Notice Search Warrant Report 2019*, U.S. Courts (Sept. 30, 2019), https://www.uscourts.gov/statistics-reports/delayed-notice-search-warrant-report-2019. Notably, the most frequently reported period of delay for delayed notice warrants, accounting for 12,096 (or 67 percent) of the applications granted, was only 30 days. *Id.*

Microsoft from providing any such notice for multiple years, it is all the more critical that the government's request for secrecy satisfy strict scrutiny. In light of the ample, longstanding precedent for the government pursuing investigations while complying with constitutional safeguards built into a variety of search and seizure mechanisms, it follows that—absent extraordinary circumstances—providing at least limited notice to the target of the SCA warrant would be consistent with decades of investigative practices.

III. Microsoft's proposed limited exception to the SCA secrecy order is a less restrictive alternative and appears to balance appropriately the interests of law enforcement and the constitutional rights of private parties.

In *amici*'s experience, years-long secrecy orders under the SCA with no exceptions are both ordinarily unnecessary and highly unusual in the context of government corporate investigations. This is especially true with regard to investigations of large, multinational companies with mature compliance functions. Typically, the fact of a corporate investigation is made apparent to its target in the early stages of an investigation through subpoenas, document requests, physical searches of offices, witness interviews, and other investigative techniques that put the company on notice of the investigation. In fact, it is difficult to conceive of an effective way to investigate the scope of culpability at a large corporation without taking such steps.

Amici understand that the relevant cloud customer in this case is a large, publicly-listed company. Appellant's Br. at 38–39, *Microsoft Corp. v. United States*, No. 20-1653(L) (2d Cir. December 7, 2020), ECF No. 98. *Amici* further understand that Microsoft has not proposed that the individuals who are the target of the government investigation receive notification of the SCA warrant, but rather argued that Microsoft be permitted to disclose the warrant *only* to a trusted individual at the target company who would be identified in consultation with the government.

As former federal prosecutors and current white-collar defense professionals, *amici* have worked closely with individuals at public companies in connection with scores of government investigations, both as government prosecutors and as defense lawyers. In particular, *amici* have worked closely with in-house lawyers and compliance professionals. Indeed, in the normal course, select personnel such as in-house lawyers are not only notified of ongoing investigations into corporate wrongdoing, but are regularly asked by the government to cooperate proactively with law enforcement by conducting internal investigations—all while protecting the confidentiality and integrity of investigations as required. In addition to employing such individuals whose jobs routinely entail appreciating and preserving confidentiality, public companies in

particular have a variety of procedures and controls designed to protect confidential information, including formal informational walls, as appropriate.

Judging from the publicly-available record, the circumstances on which the government has here relied—namely, the possibility of involvement by additional and potentially senior-level employees in the alleged wrongdoing, and the possibility of corporate criminal liability, *see* JA-87, 93, 95—are not uncommon in corporate investigations. Simply put, if those circumstances were sufficient to justify the secrecy order here at issue, then it is difficult to conceive of a corporate investigation in which such a secrecy order could not routinely issue as a matter of course—a state of affairs that would be inconsistent with the government's heavy burden under strict scrutiny analysis.

Amici's experience is consistent with the Department of Justice's own recommended practices in seeking customer data from cloud services providers:

> [A]pproaching the enterprise will often be the best way to get the information or data sought . . . . In those cases, identifying an individual within the enterprise who is an appropriate contact for securing the data is often the first step. In many enterprises, this will be the general counsel or legal representative. Counsel typically understand law enforcement needs and—perhaps more importantly—understand the importance of preserving enterprise data that has been identified as relevant to an ongoing law enforcement investigation.

U.S. Dep't of Justice, *Seeking Enterprise Data Held by Cloud Service Providers* (Dec. 2017), https://www.justice.gov/criminal-ccips/file/1017511/download (last

visited Nov. 29, 2020) ("Recommended Practices") (JA-20). *Amici* agree that "[c]ounsel typically understand law enforcement needs," particularly at large, public corporations.

Based on *amici*'s review of the record, Microsoft has proposed a practical and less restrictive alternative to the secrecy order entered by the District Court, which would satisfy the government's interest in protecting its investigation. Notifying a trusted individual at the target company of the warrant is consistent with the Department of Justice's own Recommended Practices. In *amici*'s experience, such disclosure could be made while maintaining the confidentiality of the government's investigation, particularly if the government is able to consult on the identity of such individual as Microsoft proposed here. Moreover, Microsoft's further alternative that the trusted individual would be notified solely of *the fact* of the warrant, without even being notified of the particular individuals being investigated at the large public company, would additionally mitigate concerns about compromising the integrity of the investigation. While *amici* are not privy to all information available to the parties, based on the record we have reviewed, *amici* respectfully submit that Microsoft's proposed less restrictive alternative is consistent with an appropriate balance between the interests of law enforcement and the constitutional rights of private parties. The SCA secrecy order entered by the District Court should therefore not survive strict scrutiny.

In *amici*'s experience, corporate investigations are regularly conducted through the service of grand jury subpoenas on the companies being targeted by the government. In other cases, the government will serve search warrants on the targeted companies or approach corporate employees for voluntary interviews. Notice to the corporate target is therefore the norm, and government investigators are regularly able to investigate and bring prosecutions without secrecy orders. In those cases where notice may pose some threat to an investigation, law enforcement officials have for decades conducted investigations utilizing covert methods such as wiretaps and delayed notice warrants, all of which require eventual notice to the target of the search after a reasonable time.

Careful constitutional safeguards underlying notice requirements to the target of an investigation should equally apply to searches of information maintained in the cloud. As technology advances, law enforcement must keep pace, not only in using and exploiting such technology for investigatory purposes, but also by maintaining appropriate constitutional safeguards, including those that underpin the right to notice of government searches.

CONCLUSION

For the foregoing reasons, *Amici Curiae* Former Federal Prosecutors respectfully request that the Court reverse the District Court's order denying Microsoft's motion to modify the secrecy order.

Dated: December 21, 2020
New York, New York

Respectfully submitted,

/s/ Jonathan S. Kolodner
Jonathan S. Kolodner
Rahul Mukhi
Benjamin D. Bright
CLEARY GOTTLIEB STEEN & HAMILTON LLP
One Liberty Plaza
New York, New York 10006
T: 212-225-2000
F: 212-225-3999

Edward Y. Kim
KRIEGER KIM & LEWIN LLP
500 Fifth Avenue
New York, New York 10110
(212) 390-9550

Counsel for Amici Curiae *Former Federal Prosecutors*

CERTIFICATE OF COMPLIANCE

I hereby certify that:

1. This brief complies with this Court's type-volume limitations of Federal Rule of Appellate Procedure 29(a)(5) and Local Rule 29.1(c) because it contains 3832 words, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f); and

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14 point Times New Roman font.

/s/ Jonathan S. Kolodner
Jonathan S. Kolodner

APPENDIX

Appendix of *Amici Curiae*

Jonathan S. Abernethy served as an Assistant United States Attorney for the Southern District of New York from 2001 to 2008.

Marcus Asner served as an Assistant United States Attorney for the Southern District of New York from 2000 to 2009.

Jodi Avergun served as an Assistant United States Attorney for the Eastern District of New York from 1990 to 2002.

James J. Benjamin, Jr. served as an Assistant United States Attorney for the Southern District of New York from 1995 to 2000.

Todd Blanche served as an Assistant United States Attorney for the Southern District of New York from 2006 to 2014.

David Brodsky served as an Assistant United States Attorney for the Southern District of New York from 1984 to 1991.

Jeffrey Brown served as an Assistant United States Attorney for the Southern District of New York from 2005 to 2014.

Christian Everdell served as an Assistant United States Attorney for the Southern District of New York from 2007 to 2016.

Katherine Goldstein served as an Assistant Unites States Attorney for the Southern District of New York from 2004 to 2017.

Samidh Guha served as an Assistant United States Attorney for the Southern District of New York from 2003 to 2007.

Victor L. Hou served as an Assistant United States Attorney for the Southern District of New York from 2001 to 2007.

Randall Jackson served as an Assistant United States Attorney for the Southern District of New York from 2007 to 2015.

Edward Kim served as an Assistant United States Attorney for the Southern District of New York from 2008 to 2017.

Jonathan Kolodner served as an Assistant United States Attorney for the Southern District of New York from 2000 to 2012.

Paul Krieger served as an Assistant United States Attorney for the Southern District of New York from 2008 to 2017.

Mark Lanpher served as an Assistant United States Attorney for the Southern District of New York from 2007 to 2011.

Darren LaVerne served as an Assistant United States Attorney for the Eastern District of New York from 2010 to 2016.

Andrew Levander served as an Assistant United States Attorney for the Southern District of New York from 1981 to 1985.

Nick Lewin served as an Assistant United States Attorney for the Southern District of New York from 2007 to 2017.

Rachel Maimin served as an Assistant United States Attorney for the Southern District of New York from 2010 to 2019.

Rahul Mukhi served as an Assistant United States Attorney for the Southern District of New York from 2010 to 2016.

Tai Park served as an Assistant United States Attorney for the Southern District of New York from 1989 to 1999.

Danya Perry served as an Assistant United States Attorney for the Southern District of New York from 2002 to 2013.

Ryan Poscablo served as an Assistant United States Attorney for the Southern District of New York from 2009 to 2015.

Brendan F. Quigley served as an Assistant United States Attorney for the Southern District of New York from 2012 to 2019.

Mark Racanelli served as an Assistant United States Attorney for the Southern District of New York from 2000 to 2005.

Michael Schachter served as an Assistant United States Attorney for the Southern District of New York from 1999 to 2005.

Paul Schechtman served as an Assistant United States Attorney for the Southern District of New York from 1981 to 1985 and again from 1994 to 1995.

Alexander Southwell served as an Assistant United States Attorney for the Southern District of New York from 2001 to 2007.

Charles Stillman served as an Assistant United States Attorney for the Southern District of New York from 1962 to 1966.

Jonathan Streeter served as an Assistant United States Attorney for the Southern District of New York from 2000 to 2012.

Michael Tremonte served as an Assistant United States Attorney for the Eastern District of New York from 2008 to 2011.

Jim Walden served as an Assistant United States Attorney for the Eastern District of New York from 1993 to 2002.

Justin Weddle served as an Assistant United States Attorney for the Southern District of New York from 1999 to 2014.

Jason Weinstein served as an Assistant United States Attorney for the Southern District of New York from 1999 to 2002.

Milton Williams served as an Assistant United States Attorney for the Southern District of New York from 1990 to 1994.