The Honorable James L. Robart

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

MICROSOFT CORPORATION,

Plaintiff,

v.

THE UNITED STATES DEPARTMENT OF JUSTICE, and LORETTA LYNCH, in her official capacity as Attorney General of the United States,

Defendants.

No. 2:16-cv-00538-JLR

AMICUS BRIEF ON BEHALF OF FORMER LAW ENFORCEMENT OFFICIALS IN SUPPORT OF MICROSOFT'S OPPOSITION TO MOTION TO DISMISS

***Noted on Motion Calendar*:**
September 23, 2016

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

TABLE OF CONTENTS

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

TABLE OF AUTHORITIES

Cases

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

Statutes

Other

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

IDENTITY AND INTEREST OF AMICI CURIAE

The Amici Curiae are former federal law enforcement officials in the Western District of Washington with a combined 80 years of real-life experience fulfilling their obligation to keep the public safe while operating within the bounds of the Constitution. They have a unique perspective on how to achieve the balance between public safety and personal liberty, particularly with respect to government searches and seizures of private information. They respectfully offer that perspective in the hopes of assisting the Court understand that law enforcement can function effectively—even in the cloud—while following the Fourth Amendment's requirement of notice to individuals whose private information has been searched.

Amici are cognizant of the increasing challenges to law enforcement in the digital age. They understand and agree that specific circumstances, like the safety of a witness or operational integrity, can justify and require delaying notice to targets of an investigation. But as discussed below, that should require a specific and meaningful showing that such an exigency exists, and the delay should be limited in duration.

Jeffrey Sullivan was the U.S. Attorney for the Western District of Washington from 2007 to 2009. Sullivan also served as the Yakima County Prosecuting Attorney for 27 years.

John McKay was the U.S. Attorney for the Western District of Washington from 2001 to 2007.

Kate Pflaumer was the U.S. Attorney for the Western District of Washington from 1993 to 2001.

Mike McKay was the U.S. Attorney for the Western District of Washington from 1989 to 1993. McKay also served as a Senior Deputy Prosecuting Attorney for King County for five years.

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

Charles Mandigo was the Special Agent in Charge of the FBI's office in Seattle from 1999 to 2003. Before retiring in 2003, he worked for the FBI for 28 years, including in New York, Chicago, and at FBI Headquarters.

Both parties have consented to the filing of this amicus brief. Amici have also filed a motion for leave to file this brief, consistent with this Court's Order on the filing of amicus briefs (Dkt. 42).[1]

I. INTRODUCTION

The Fourth Amendment protects all of us from unreasonable searches and seizures of private information. "The security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society." *Wolf v. Colorado*, 338 U.S. 25, 27 (1949). Law enforcement officials are charged with supporting and defending that right.

The balance between individual liberty and public safety in the context of emerging technologies is not new to the courts. What started with cameras, telephones, and recording devices has evolved into computers, smart phones, and the cloud. Each new technology requires an equivalent application of the bedrock Fourth Amendment principles that law enforcement officials have operated under for decades. The Fourth Amendment "must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." *United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010). The "broad and unsuspected governmental intrusions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." *United States v. U.S. Dist. Court for E.D. Mich.*, 407 U.S. 297, 313 (1972) (footnote omitted).

[1] Amici state that neither a party nor a party's counsel authored this brief in whole or in part, and no person (including a party or its counsel), other than amici or their counsel, contributed money intended to fund preparing or submitting this brief. John McKay is a partner at Davis Wright Tremaine LLP, which is representing Microsoft in this matter. He joins this brief in his personal capacity as a former law enforcement official.

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

In the face of ever advancing technology, Amici respectfully submit that law enforcement officials have functioned—and can continue to function—effectively under the constitutional rule that the Fourth Amendment requires notice to the target of the government's search. There are narrow exceptions to that rule when the particular facts of the case demand it. In those cases, notice to the target may be delayed for a reasonable period, but not abandoned entirely. In the Ninth Circuit, for 30 years, the permissible delay has been seven days, with longer periods of delay allowed, but only "upon a strong showing of necessity." *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986). Law enforcement officials are accustomed to making particularized showings to defer notice of searches in both the physical and electronic world. They can continue to do so in the cloud.

II. ARGUMENT

A. An essential function of a warrant is to provide notice to the target of a government's search which, in turn, serves important interests.

The Fourth Amendment requires that government searches be reasonable. A hallmark of reasonableness is law enforcement's obtaining a warrant from a neutral magistrate. "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). That notice is vital. Obtaining a warrant, but not disclosing it, nullifies an essential function of the warrant, which is to provide notice to the person who is the target of the search. Moreover, non-disclosure of searches has a broader effect on the criminal justice system that undermines the balance between public safety and personal liberty.

An "essential function of the warrant 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. Williamson*, 439 F.3d 1125, 1132 (9th Cir. 2006) (quoting *United States v. Chadwick*, 433 U.S. 1, 9 (1977)) (emphasis added). A "major function of the warrant is to provide *the property owner* with sufficient information

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

to reassure him of the entry's legality." *Michigan v. Tyler*, 436 U.S. 499, 508 (1978) (emphasis added).

For the individuals deprived of notice, they "will never know that [the government] chose not to provide notice to them," and thus "have no opportunity to challenge the government's failure to give notice, let alone the legality of the underlying search." Patrick Toomey & Brett Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, and the Right to Notice*, 54 SANTA CLARA L. REV. 843, 848 (2014). That not only erodes the public's trust in law enforcement, it also deprives the judicial branch from serving as a check on executive power. As one commentator, who is also a magistrate judge and thus on the front lines of issuing warrants and electronic surveillance orders, has observed, "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).

He further explained, "[l]ack of appellate review is unhealthy for any regulatory scheme, especially one designed to check executive power. Every statute has its rough edges of ambiguity and gaps of uncertainty. These flaws are brought to light and repaired, day by day, case by case, through lower court rulings subject to review and correction by the courts of appeal, and, ultimately, by the Supreme Court." *Id.* at 331.[2] Without that, 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 process." *Id.*; *see also In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp.

[2] None of that is to suggest that a facial challenge is inappropriate here. Rather, Microsoft is challenging—and Amici support its challenge—a statutory scheme that prevents individuals from receiving notice that would allow them to challenge the lawfulness of a government's search, which, in turn, allows for the day by day, case by case review necessary for effective judicial oversight.

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

2d 876, 895 (S.D. Tex. 2008) (Smith, M.J.) ("As a rule, sealing and non-disclosure of electronic surveillance orders must be neither permanent nor, what amounts to the same thing, indefinite."). Law enforcement officials—and the entire criminal justice system—benefit from that judicial oversight and guidance, including the review provided by district courts of orders by magistrate judges.

Finally, providing notice of a search also serves a fundamental goal of law enforcement officials: maintaining the public's faith in them. Giving notice helps "head off breaches of the peace by dispelling any suspicion that the search is illegitimate." *United States v. Gantt*, 194 F.3d 987, 1002 (9th Cir 1999) (quotations omitted). Leaving the public in the dark regarding governmental intrusion into individuals' private effects and communications, does not, in the long run, foster trust in the law enforcement community. Rather, indefinite secrecy increases public suspicions that government searches are illegitimate. Without the public's confidence, law enforcement officials struggle with their mission to keep order.[3]

B. Because covert searches raise serious constitutional concerns, they are allowed only when the facts of a particular case demand it and notice is delayed—*not* abandoned.

The Fourth Amendment does not prohibit *all* covert searches. *Dalia v. United States*, 441 U.S. 238, 247 (1979). Effective law enforcement efforts often require some measure of secrecy during an investigation to avoid alerting a target, who might destroy evidence or flee. But covert searches raise significant constitutional concerns that Congress and the courts recognize by establishing strict parameters and reasonable after-the-fact notice requirements. The law enforcement community has operated effectively within those parameters for decades. It can continue to do so in the cloud.

---

[3] Amici focus in this brief on the requirements of the Fourth Amendment. But they recognize the compounding effect of the non-disclosure orders authorized by 18 U.S.C. § 2705(b), which creates a situation in which the government need not provide notice of its search *and* can compel a provider like Microsoft to stay silent about the search indefinitely.

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

1. Wiretaps and bugging equipment.

When the government wants to listen to a person's conversations, it must obtain a warrant, although it may delay providing notice of the warrant and search to avoid alerting the targets. Two features of the federal statute authorizing the interception of wire, oral, or electronic communications (18 U.S.C. § 2518)—and key to its constitutionality—are a showing of special facts justifying the search and eventual notice to the target of the search. The Supreme Court struck down a state wiretapping statute because it had "no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts." *Berger v. New York*, 388 U.S. 41, 60 (1967). 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.*

In contrast, the Supreme Court upheld the constitutionality of the federal statute authorizing covert wiretapping because it "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)). The Court also upheld the constitutionality of covert entries into private premises to install electronic bugging equipment for recording conversations on the same grounds. *Id.* at 247-48. The Court recognized that "electronic surveillance can be a threat to the cherished privacy of law-abiding citizens unless it is subjected to the careful supervision prescribed by" the statute. *Id.* at 250 n.9. But that the "detailed restrictions" of the statute "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.

The statute requires the government to establish, among other things, that there is probable cause to believe that an individual has committed a crime; that particular

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

communications concerning that offense will be obtained through interception; and that normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous. 18 U.S.C.§ 2518(1). The statute provides for notice of searches "[w]ithin a reasonable time but not later than ninety days." *Id.* § 2518(8)(d). And notice is not limited to the target of the search, but may also go to "other parties to intercepted communications as the judge may determine … is in the interest of justice." *Id.* The combination of the government's showing a particularized need, plus eventual notice of the search to the target, allow the statute to pass constitutional muster.

2. "Sneak-and-Peek" warrants / delayed notice searches.

Courts have also upheld the constitutionality of so-called "sneak-and-peek" warrants that permit law enforcement to enter and examine an area, take an inventory, and then leave without disturbing the contents or notifying the person whose effects were searched. "Lack of seizure explains the 'peek' part of the name; the 'sneak' part comes from the fact that agents need not notify the owner until later." *United States v. Mikos*, 539 F.3d 706, 709 (7th Cir. 2008). "Such warrants are designed to permit an investigation without tipping off the suspect." *Id.* They are also called "delayed notice" searches.

The Ninth Circuit has authorized delayed notices searches, but, at the same time, recognized their dangers: "surreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment." *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986). Because of those risks, the Court imposed restrictions on delayed notice searches, principle among them the requirement of prompt notice. "[T]he Fourth Amendment requires that officers provide notice of searches within a reasonable, but short, time after the surreptitious entry." *United States v. Johns*, 948 F.2d 599, 605 n.4 (9th Cir. 1991). Thus, the government may delay notice of a sneak-and-peek search, but the delay "*should not exceed seven days except upon a strong showing of necessity*." *Freitas*, 800 F.2d at 1456 (emphasis added).

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

In *Freitas*, the Court noted that the federal wiretapping statute, discussed above, "makes clear the constitutional importance of *both* the *necessity* for the surreptitious seizure *and* the *subsequent notice*." 800 F.2d at 1456 (emphasis added). And while the Court suggested that a showing of necessity "could have strengthened the claim" that the sneak-and-peek search was constitutional, it was "clear that the absence of any notice requirement in the warrant cast[ed] strong doubt on its constitutional adequacy." *Id.* As a noted commentator observed about *Freitas*, "[i]t is to be doubted … that a showing of necessity for surreptitious entry would excuse a *total* failure to give the occupant a post-search notice of the warrant execution." 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.7(c) (5th ed. 2012); *see also* Toomey & Kaufman, 54 SANTA CLARA L. REV. at 855 (under existing case law "the idea that notice of the search may be dispensed with altogether is simply off the table"). In other words, the Fourth Amendment allows delayed notice—not *abandoned* notice.

The Ninth Circuit re-affirmed its holding in *Freitas* and applied its notice requirement to sneak-and-peek searches of a person's effects in an off-site storage facility. *United States v. Johns*, 851 F.2d 1131, 1134-35 (9th Cir. 1988); *Johns*, 948 F.2d at 605 n.4. In the *Johns* decisions, there was no indication that the government could have by-passed the Fourth Amendment simply by providing notice of the search to the owner of the storage facility. Those decisions have important implications for the government's position in this matter regarding the adequacy of providing notice of the search to Microsoft, i.e., the owner of the off-site storage facility, not the person whose information has been searched.

In 2001, Congress codified delayed notice search warrants. 18 U.S.C. § 3103a. When applying for a warrant under the statute, the government may ask the court for permission to temporarily delay notice that a warrant has been executed upon a showing of "reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result," and, in the case of a delayed notice seizure, a showing

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

of "reasonable necessity for the seizure." *Id.* § 3103a(b)(1)&(2). Similar to earlier case law, the statute requires notice of the search, but allows notice to be delayed for a "reasonable period" of time specified *in the warrant* and "not to exceed 30 days after the date of its execution, or on a later date certain if the *facts of the case* justify a longer period of delay." *Id.* § 3103a(b)(3) (emphasis added). No delay of notice beyond the time specified in the warrant is allowed without further court authorization, with good cause shown and upon "an *updated* showing of the need for further delay and that each additional delay should be limited to periods of 90 days or less, unless the *facts of the case* justify a longer period of delay." *Id.* § 3103a(c) (emphasis added).

The statute also includes reporting requirements such that a court must report the issuance or denial for a delayed notice search warrant, including the offense specified in the warrant or application, the period of delay authorized, and the number and duration of any extensions. 18 U.S.C. § 3103a(d)(1). The reporting requirement provides information to policy makers and the public as to how often and for what purposes the government is conducting delayed notice searches. That, in turn, allows for transparency, at least in the aggregate, of law enforcement's use of the statute's procedures.

C. Law enforcement officials can operate effectively within parameters that require particularized showings and eventual notice to search targets.

Law enforcement officials have decades of experience operating within the parameters of making particularized showings and delaying—but not dispensing with—notice of searches. Congress enacted the wiretapping statute in 1968, which means law enforcement officials nationwide have functioned within its limits for almost 50 years. Further, law enforcement officials in the Ninth Circuit have operated effectively within the parameters of *Freitas*'s seven-day delayed notice default rule for 30 years. Longer periods of delay are allowed, but only "upon a strong showing of necessity." *Freitas*, 800 F.2d at 1456. A "strong showing of necessity" surely must be more than a rote recitation of the

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

statutory elements constituting an "adverse result," and instead require a case-specific showing.

Section § 3103a provides for a 30-day delay of a search warrant, but any delays beyond 30 days must be justified with a particularized showing grounded in "facts of the case." Congress did not do away with notice entirely. In a 2004 report to Congress, the U.S. Department of Justice emphasized how workable delayed notice warrants were—and that they were used "infrequently and judiciously." U.S. Dep't of Justice, *Delayed Notice Search Warrants: A Vital and Time-Honored Tool for Fighting Crime*, at 4, 8, Sept. 2004, *available at* https://www.justice.gov/sites/default/files/dag/legacy/2008/10/17/patriotact213report.pdf.

The number of applications for delayed notice search warrants has increased since then. Over a one-year period ending September 2014, prosecutors made 7,627 delayed notice warrant requests and 5,243 requests for extensions. Report of the Director of Administrative Office of the United States Courts on Applications for Delayed-Notice Search Warrants and Extensions, at 1, 2014, *available at* http://www.uscourts.gov/statistics-reports/analysis-reports/delayed-notice-search-warrant-report. That averages to 81 delayed notice search warrants for each of the 94 federal district courts over a one-year period, or 6.7 per month. The most frequently reported period of delay was 90 days. *Id.* at 2.[4] Of greater relevance, Microsoft here suggests that a review of orders it has received indicates that the standard practice in particular U.S. District Courts is to set definite time limits on the § 2705(b) orders that preclude it from notifying customers of a search. *See* Microsoft's Opp. to Government's Mot. to Dismiss, at 13 n.10 (Dkt. 44).

[4] The data include delayed notice searches not just of homes and businesses, but also cell phone location tracking, GPS tracking, and searching emails, which helps explain the increase in applications since 2004. Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment "Rule Requiring Notice,"* 41 PEPP. L. REV. 509, 542-44, 531, 539-49 (2014) (increasing judicial pressure on the government to use search warrants for searches that had previously been conducted without a warrant, like cell phone location tracking, GPS tracking, and email searches, has likely driven the increase in applications under § 3103a).

YARMUTH WILSDON PLLC
1420 FIFTH AVENUE, SUITE 1400
SEATTLE WASHINGTON 98101
T 206.516.3800 F 206.516.3888

All that is meant to show that the law enforcement community has lived with delayed notice searches, and the restraints around them, for decades. They can operate effectively within those parameters in the cloud, too—not because it is easy, but because the Fourth Amendment requires it.

III. CONCLUSION

Some commentators have warned of the risk of delayed notice searches, noting that "[w]ith traditional searches, each person in the community knows when and if her home or business has been searched by the government. … The privacy intrusion of these searches is deep but narrow—deep in the sense that one's home has been searched, and narrow in the sense that the invasion impacts only those few who are searched. With delayed notice searches, however, every member of the community suffers a more indirect and uncertain loss of privacy." Witmer-Rich, 41 PEPP. L. REV. at 555-56. The Ninth Circuit recognized those risks in *Freitas* and *Johns* and established a seven-day delay default rule. But however great the perils of delayed notice searches are, the risks posed by no-notice searches are greater. And for no good reason. Law enforcement officials have no practical need to keep their searches secret indefinitely, except in the rarest of circumstances, which must be supported by particularized need. For the foregoing reasons, Amici respectfully request that the Court deny the government's motion to dismiss Microsoft's complaint.

DATED this 2nd day of September, 2016

YARMUTH WILSDON, PLLC

By: *s/ Kristina Silja Bennard*
Kristina Silja Bennard, WSBA # 37291
1420 Fifth Avenue, Ste. 1400
Seattle, WA 98101
T: 206.516.3800
F: 206.516.8888
Email: kbennard@yarmuth.com

Attorneys for Amici Curiae Former Law Enforcement Officials

CERTIFICATE OF SERVICE

I hereby certify that on September 2, 2016, I electronically filed the foregoing **AMICUS BRIEF ON BEHALF OF FORMER LAW ENFORCEMENT OFFICIALS IN SUPPORT OF MICROSOFT'S OPPOSITION TO MOTION TO DISMISS** with the Clerk of the Court using the CM/ECF system, which will send notification of each filing to those attorneys of record registered on the CM/ECF system.

DATED this 2nd day of September, 2016.

YARMUTH WILSDON, PLLC

By: *s/ Kristina Silja Bennard*

Kristina Silja Bennard, WSBA # 37291
1420 Fifth Avenue, Ste. 1400
Seattle, WA 98101
T: 206.516.3800
F: 206.516.8888
Email: kbennard@yarmuth.com