Written Testimony of Tom Burt
Corporate Vice President, Customer Security & Trust
Microsoft Corporation

United States House Committee on the Judiciary
Hearing on "Secrecy Orders and Prosecuting Leaks: Potential Legislative Responses to Deter Prosecutorial Abuse of Power"

June 30, 2021

Chairman Nadler, Ranking Member Jordan, and Members of the Committee, my name is Tom Burt and I am the Corporate Vice President for Customer Security & Trust at the Microsoft Corporation. My team works to ensure customer trust in Microsoft's products and online services, and it includes our Law Enforcement and National Security team, which is responsible for responding to lawful access requests for customer data from governments around the world. I want to thank you for the opportunity today to provide Microsoft's perspective on the overuse of secrecy orders and the need for legislative reform.

The recent revelations that the Justice Department secretly targeted journalists and Members of Congress, their staff, and even their families with secret legal demands for their sensitive personal data were shocking to many Americans. But what may be most shocking is just how routine court-mandated secrecy has become when law enforcement targets Americans' emails, text messages, and other sensitive data stored in the cloud.

I want to be clear: The overuse and abuse of secrecy orders is not new, and in fact it has remained an ongoing problem since the ascendancy of cloud computing. It is not unique to one administration or political party. And it is certainly not limited to investigations targeting the media and Congress. Secrecy orders under 18 U.S.C. § 2705(b) — also known as non-disclosure orders — have unfortunately become commonplace. They are often approved even for routine investigations without any meaningful analysis of either the need for secrecy or the orders' compliance with fundamental constitutional rights.

Some may mistakenly assume that total secrecy is a standard feature of law enforcement investigations. But that has never been the case. Before the cloud, law enforcement agents executed search warrants and subpoenas seeking someone's personal correspondence and documents by serving them directly on the people or organizations they wished to search — in other words, the targets received notice. Law enforcement has historically functioned this way and done so with success.

In recent years, law enforcement has taken advantage of the efficiencies made possible because of the expansion of cloud computing and technology. As users have moved their email, photos and other data to the cloud, they should have the benefit of an increased expectation of privacy for that data as the cloud is much more secure than any internet connected computer in any home, business, or organization. But for citizens, businesses and organizations throughout America, this expectation of privacy is unknowingly misplaced. Their own government is secretly demanding users' data, without their knowledge, from cloud service providers, exploiting a subsection of the 35-year-old Electronic Communications Privacy Act to prevent notification of the demand to users by the cloud service providers. By doing so, the government has transformed decades-old criminal investigative techniques into secret surveillance operations — all without rigorous review by courts. This lack of transparency inevitably leads to overuse and abuse, such as the recently revealed subpoenas of data belonging to journalists and legislators.

Secret investigations: Once the exception, now a norm

Traditionally, secrecy was the exception. In recent years, law enforcement has turned that exception on its head, developing a practice of reflexively asking to keep even routine investigations secret. Providers, like Microsoft, regularly receive boilerplate secrecy orders unsupported by any meaningful legal or factual analysis.

While a few courts have criticized the government for submitting boilerplate applications,[1] there is significant evidence that courts do not regularly hold the government to any meaningful standard when determining, in secret ex parte hearings where only prosecutors are present, whether the requisite showing for secrecy has been made. Secrecy orders signed by judges typically include only a cursory assertion that the government has satisfied any or all of the statutory factors authorizing secrecy.[2] The Justice Department's own template for a surveillance order application under 18 U.S.C. § 2703(d) does not even require a prosecutor to provide facts justifying the need for secrecy. The template merely blindly asserts that any disclosure would "seriously jeopardize" the investigation for a variety of boilerplate reasons.[3]

It is no surprise, then, that such secrecy orders have become routine. At Microsoft, we are committed to transparency. Twice a year we release a public report that provides an extraordinarily close look at the legal demands we receive from law enforcement agencies around the world. We also fought in court for the right to publicly report on national security demands we receive each year — a right that this Committee helped to codify in the USA FREEDOM Act of 2015.

We have reviewed the number of secrecy orders that federal law enforcement agencies have presented to us from 2016 to the present, a period that spans the Obama, Trump, and Biden administrations. We found that while the number has increased some, federal law enforcement has consistently presented us with 2,400 to 3,500 secrecy orders each year, or 7-10 per day,

---

[1] "In each [of 15 separate applications seeking a secrecy order], the application relies on a boilerplate recitation of need that includes no particularized information about the underlying criminal investigation. For the reasons set forth below, I now deny each application without prejudice to renewal upon a more particularized showing of need. . . ." *In re Grand Jury Subp. Subp. to Facebook*, 2016 WL 9274455, at *1 (E.D.N.Y. May 12, 2016). *See also, e.g., In re Subp*., 2018 WL 565004, at *2 (D. Nev. Jan. 25, 2018) ("The application as currently submitted fails to establish sufficient grounds for a non-disclosure order. First, a particularized showing of need has not been made and, instead, the application rests on boilerplate assertions that could be made with respect to essentially any grand jury proceeding.").

[2] Under 18 U.S.C. § 2705(b), a court shall enter a secrecy order if it determines there is reason to believe that notification of the underlying legal process will result in (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses; or (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

[3] The template states: "The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), ISPCompany be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this Order for such period as the Court deems appropriate. The United States submits that such an order is justified because notification of the existence of this [underlying surveillance] Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution." *See* "Sample 18 U.S.C. § 2703(d) Application and Order," Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Manual (2009).

representing one-quarter to one-third of all the legal demands we received. These are just the demands that Microsoft, just one cloud service provider, received. Multiply those numbers by every technology company that holds or processes data, and you may get a sense of the scope of the government's overuse of secret surveillance.

The fact that law enforcement requested, and courts approved, clandestine surveillance of so many Americans represents a sea-change from historical norms. If law enforcement wants to secretly search someone's *physical* office, it must meet a heightened burden to obtain a sneak and peak warrant. More specifically, law enforcement has to prove to a judge with specific and articulable facts that a secret warrant is necessary and Congress placed a strict, presumptive 30-day limit on the length of time that secrecy may last. However, if they want to search your *virtual* office, they just serve a simple warrant on your cloud provider and obtain secrecy through a boilerplate process. Just a decade ago, in 2010, federal judges approved fewer than 2,400 requests for sneak and peak warrants nationwide[4] — a smaller amount than the number of secrecy orders that Microsoft alone received in any of the last five years.

Microsoft does not simply comply with such demands without question. We review them closely to protect our customers' interests. Some of the demands Microsoft received were legally deficient and we did not comply. In other cases, we have challenged — through negotiation or litigation — the orders. This includes secrecy orders approved by courts where the account holder was not a target of the investigation but a victim; where the investigation related to just one email account belonging to a large, reputable organization — a company, government, or school — and there was no allegation that the organization itself or its leadership was suspected of wrongdoing; where the government was engaged in discovery negotiations with an organization under investigation, and then secretly demanded the very same records from us to evade a dispute over privilege and the extent of discovery; and even where the owner of the target account consented to the search.

Our record challenging unnecessary secrecy

In fact, Microsoft has a long history of successfully challenging unnecessary secret surveillance, both directly in conversations with law enforcement and formally in court. Often, law enforcement will realize its secrecy demand lacks justification and will agree to let us provide advance notice to the owner of the target account. Sometimes law enforcement authorities even concede they came to us because it was simply "easier." Of course, "easier," is not, and should never be, the basis for a secrecy order.

When we cannot come to an arrangement with the government that allows us to provide advance notice, sometimes we challenge secrecy orders in court. In 2014, we sued the federal government to allow us to notify a customer who was targeted with a National Security Letter. The government eventually withdrew the demand and went to the customer directly for the information. In 2016, Microsoft brought a declaratory judgment action, asking a federal district

[4] Report of the Director of the Administrative Office of the United States Courts on Applications for Delayed-Notice Search Warrants and Extensions, 2010, *available at* https://www.uscourts.gov/sites/default/files/2010_delayed_notice_search_warrant_report_0.pdf.

court to find that indefinite secrecy orders are unconstitutional. In response, the Justice Department issued guidance intended to limit secrecy orders to one year. In two cases unsealed just this year, the government relented to our requests and agreed to allow notice to our customers after we filed suits in court. And just last month, while preparing for oral argument in a case before the Second Circuit, the Justice Department asked the court to vacate another secrecy order we had challenged and to dismiss the case as moot. While our company has had success challenging secrecy orders in the courts, we have found that these individual challenges do not stem the tide of unnecessary secrecy orders. Litigation is no substitute for legislative reform.

Many of these orders should never have been approved by the courts. The current rubberstamping process places the onus on providers to challenge inappropriate secrecy orders. But providers have access to only the very limited information included in the secrecy order and underlying legal process, leaving providers in the dark about the supposed factual bases underlying the purported need for secrecy. We often have no idea, and no way to learn, whether the secrecy order is one of the very few that are truly justified, or not.

These problems are compounded for orders impacting consumer accounts. Consumer email addresses are generally anonymous. When Microsoft received one of the secret subpoenas that we now know targeted a congressional staffer in 2017, we were not aware of who the individual was or what the subpoena concerned. The laws and Justice Department policies did not require the government to provide us with any such information about the demand. It was only after the secrecy order expired and Microsoft – not the government – notified the individual about the subpoena that we learned about the troubling circumstances at issue.

A path forward

Thirty-five years ago this month, this very Committee held a markup and reported out the bill that governs secret electronic surveillance orders. The Electronic Communications Privacy Act became law at a time when only a tiny fraction of Americans had personal computers. We were still years away from a rudimentary at-home internet. Congress simply could not have envisioned modern cloud computing, or how our most basic and fundamental concepts of privacy have become wholly dependent on the security of our data in the cloud.

It's time for this Committee to update this antiquated law. The time is right to reform secrecy orders to prevent their overuse and abuse. Only a few key changes are necessary to protect the rights of Americans from unwarranted secret surveillance.

The reform principles we are proposing would not prevent secrecy when truly necessary to protect an investigation. Rather, they would require judges to carefully consider, based on an individualized factual showing, whether to approve a secrecy order. These reforms would bring the statute in line with how searches are conducted in the physical world. They would bring the statute in line with the Constitution. And they would expand on important secrecy order reforms contained in prior, broader ECPA reform efforts that Microsoft has supported for years.

First, Congress should end indefinite secrecy orders for good. One of Microsoft's lawsuits resulted in a new Justice Department policy in 2017 that was intended to limit secrecy orders to one year; unfortunately, we continue to receive federal orders approved with no expiration date at all. We suggest that secrecy orders be limited to a reasonable time, such as 90 days, with extensions of the same length available when the continued need for secrecy is justified based on articulated facts and approved by a judge.

Second, we believe the government should be required to provide notice to the target of a demand for data upon the expiration of a secrecy order. While Microsoft makes these notifications now, it is unclear whether all providers follow the same practice. Moreover, ensuring the fundamental right to know when a person's virtual office or virtual data has been searched should not be left to the vagaries of companies' preferences and processes, but should occur uniformly by the very government who executed the covert search.

Third, Congress must make the standard to obtain a secrecy order meaningful. To address the trend of boilerplate motions and orders, we suggest that courts be required to find, based on specific and articulable facts and documented in their written findings, that one of the current statutory factors for secrecy is likely met, replacing the statute's current nebulous "reason to believe" standard. Simply requiring a full, meaningful, reviewable written analysis will have an enormous impact on the decision making of both the Justice Department and the courts.

Fourth, the standard for a secrecy order must also be made consistent with the First Amendment. Courts have rightly held that a secrecy order is a government mandate that a provider refrain from exercising its freedom of speech, and that providers can challenge secrecy orders under the First Amendment.[5] But courts have not traditionally applied the First Amendment strict scrutiny standard when *issuing* the secrecy order; they have applied this standard only when considering a challenge after the fact, approving countless orders without any meaningful First Amendment review. We suggest that Congress close this constitutional loophole by requiring courts to find, before approving a secrecy order, that the order is narrowly tailored to achieve a compelling government interest, consistent with the First Amendment.

Fifth, providers have seen too many examples of the government preventing notification of a demand to a large organization or university when only one employee or student's email account is being searched, and when the organization is not suspected of any wrongdoing. This appears to be what happened to Google with *The New York Times* investigation. Before cloud computing, these organizations would have received court orders directly, and there is simply no justification to keep them in the dark just because they use the cloud. Google rightly pushed back, and we do, too. But providers should not be the only ones standing up for the constitutional rights of those impacted by government surveillance. When approving an order, courts should find that no one representing the company, school, or other organization on whose domain the data is hosted could be notified without an adverse result under the statute occurring. Simply requiring a judge to ask that question will prevent numerous inexcusably overbroad secrecy orders.

[5] *See, e.g., Microsoft Corp. v. United States Dep't of Justice*, 233 F. Supp. 3d 887, 900 (W.D. Wash. 2017); see also *Matter of Search Warrant for [redacted].com*, 248 F. Supp. 3d 970, 980 (C.D. Cal. 2017).

Sixth, we need more transparency around secrecy orders, both in terms of their overall use and the information providers and users can access to allow them to properly consider their rights when confronted with an order.

Finally, despite the undeniable impact of secrecy orders on the rights of both providers and our customers, some courts have found that providers lack standing to challenge such orders. We suggest that Congress codify a statutory right to allow providers to intervene to challenge harmful secrecy orders, to protect their users and to ensure the statutory and constitutional requirements are met.

These reforms, taken together, would serve as a strong foundation for ending the abuses of secrecy orders that Microsoft and other technology providers see each day. At the same time, it would enable the issuance of properly narrow, time limited and factually justified secrecy orders when truly necessary to protect a criminal investigation.

In closing

Before I close, I also want to reiterate that we do not oppose all secrecy orders. We cooperate with the Justice Department to investigate criminal and national security cyber-attacks, to keep our children safe from online exploitation, to disrupt criminal enterprises, and to prevent terrorist attacks. In fact, through our Digital Crimes Unit we actively work, together with law enforcement, to deter or prevent such crime. Certain sensitive investigations merit non-disclosure orders. We are not suggesting that secrecy orders should only be obtained through some impossible standard. We simply ask that it be a meaningful one.

Government accountability depends on transparency. That concept is central to our democracy. Secrecy should be the rare exception, not the norm. Providing notice to an individual the government targets with a warrant or other demand for information is a critical protection against government overreach. Safeguarding one's constitutional rights requires knowledge that those rights are at risk. Without notice, an individual is left in the dark, unable to raise privileges or other objections that may be applicable, and unable to protect their rights in court. Reform is necessary to protect the reasonable privacy expectations and rights of the press, our legislators, their staff and their families. It is needed to protect all of Microsoft's customers and the customers of other cloud service providers. It is needed to protect fundamental values that are the bedrock of our democracy.

Through our advocacy here in Congress, in the courts, and with law enforcement, Microsoft will continue to do everything it can to prevent the misuse of secrecy orders. But we respectfully request that you work with us to fully address this problem. Without legislative reform, abuses will continue to occur — and they will continue to occur out of sight.

Thank you for your time and attention.

# # # # #