# DC Circ. Ruling Augurs More Scrutiny Of Blanket Gag Orders

By **Gregory Rosen** (August 13, 2025)

Gregory Rosen

In an era when vast amounts of personal data are stored online and frequently sought by federal investigators, the government has relied heavily on nondisclosure orders, or NDOs, to keep its subpoenas secret.

More recently, the government has sought something more comprehensive in scope: an omnibus NDO.

An omnibus NDO is a type of court order that prohibits the recipient — usually a service provider, witness or company — from disclosing the existence or contents of one or more legal demands, including subpoenas, search warrants or other compelled disclosures.

Omnibus NDOs are unique insofar as they do not apply to a single subpoena; rather, they can be tailored to a broader investigation, covering all similarly situated requests issued. They are generalized in scope and can be extensive in duration, but are less individually tailored to a specific legal request.

Omnibus NDOs can be key to a prosecution: Instead of having to obtain separate legal process for every single subpoena or warrant, the government can protect a wide array of information from outside disclosure.

For example, while investigating a drug cartel within the U.S., law enforcement officials may learn that the overall enterprise continuously uses cellphones through the usual and known carriers. An omnibus NDO would allow a federal prosecutor or investigator to protect the integrity of the investigation when issuing subpoenas to multiple carriers, so long as the order itself is tailored to the broader drug cartel investigation and justified in writing.

Because of their wide-ranging nature and long duration, omnibus NDOs have come under increasing scrutiny by the private sector. Detractors argue their breadth may violate the First Amendment rights of companies or people, and have raised concerns over whether the government's requests contain sufficient justification to deprive an individual from releasing investigative information.

On July 18, the U.S. Court of Appeals for the District of Columbia Circuit handed a win — albeit a narrow one — to those detractors on the latter issue. In In re: Sealed Case, the court rejected a government attempt to use a yearlong, forward-looking NDO regime without the required judicial findings.[1]

The ruling is a wake-up call to prosecutors, and provides a road map for private parties pushing back on overbroad secrecy demands.

**The Case**

Under the Stored Communications Act, the government may apply for a court order preventing a service provider from disclosing that it received a subpoena.[2] But the statute is clear: A court may issue such an order only if it determines that disclosure "will result in" a specific harm, such as destruction of evidence or jeopardizing an investigation.[3]

In In re: Sealed Case, the U.S. Attorney's Office for the District of Columbia sought something broader. Instead of applying for an NDO tied to a particular subpoena, the government asked a magistrate judge to approve a blanket order authorizing the attachment of nondisclosure language to any subpoena issued over a one-year period in a particular investigation — the details of which remain under seal, as the case name suggests.[4]

The magistrate judge granted the request and effectively allowed the government to self-certify, in each future instance, whether the subpoena met the statutory standard for nondisclosure.

This was not a novel NDO request. Indeed, omnibus NDOs have provided tremendous utility to government prosecutors, helping to issue legal process efficiently and quickly, without technical interruptions. As we see in the D.C. Circuit's decision, however, technicalities matter.

When X Corp. — formerly Twitter — was served with this subpoena and accompanying NDO, it moved to vacate the order.[5] The U.S. District Court for the District of Columbia upheld the NDO, relying on ex parte evidence.[6]

X appealed, which led to the D.C. Circuit's July 18 reversal. The panel held that the district court failed to comply with the plain language of Title 18 of the U.S. Code, Section 2705(b), which requires the court to determine whether disclosure will result in a statutorily enumerated harm. By allowing the government to make that determination on its own, the magistrate had unlawfully delegated a judicial function to the executive branch.

As noted by the D.C. Circuit:

> If the order covers just one subpoena that is before the court, the inquiry is straightforward. ... If the order covers multiple subpoenas, though, the court must make a determination that addresses all those subpoenas. Similarly if the order applies to future, hypothetical subpoenas, the court ordinarily must identify the types of subpoenas to which its order can apply so it can explain why it has reason to believe disclosure of those potential subpoenas will cause harm.[7]

The court further noted the lack of transparency in the order about the would-be recipients of the future subpoena. According to the opinion, government requests may not necessarily be targeted to putative defendants, but could be issued to peripheral witnesses. "To satisfy the statute," the D.C. Circuit wrote, "the court needed to acknowledge the potential variety in the subpoenas … [o]nly then could it have" established a future risk of harm.[8]

Importantly, the D.C. Circuit emphasized that it was not categorically barring all multisubpoena or prospective NDOs.[9] But it made clear that any omnibus NDO must be tightly tailored and supported by judicial findings that account for the scope, variety and timing of the subpoenas involved.

Specifically, the D.C. Circuit found that the judge issuing the order must explain why disclosure might harm the investigation "during the next year," recognizing that facts may change — e.g., the public may learn about what's happening[10] — or "the target of the subpoena or investigation could be taken into custody or pass away, eliminating any risk."[11]

In other words, the D.C. Circuit told prosecutors they must cross their t's and dot their i's. And while the court declined to categorically bar omnibus orders — indeed, it confirmed that using a single order to apply to multiple subpoenas would be well within the wheelhouse of the statute — in a broader investigation, the government must justify, with more detail and legal bases, why the risk is worth the nondisclosure, and if so, how. And the issuing court must, in turn, make those requisite findings.

**Future Implications**

The In re: Sealed Case ruling puts prosecutors on notice. Omnibus NDOs may still be viable tools in complex or fast-moving investigations, but only if the government can show, up front, that each category of covered subpoena poses a real risk of harm. Boilerplate assertions or reliance on investigative efficiency won't cut it.

Instead, courts will require a meaningful explanation from federal prosecutors and law enforcement of why secrecy is necessary for each future subpoena, alongside more clearly defined categories of subpoenas. The government must justify why a forward-looking NDO is appropriate generally in light of possibly changing facts and circumstances, and the court issuing the order should consider clear limits on the NDO's temporal and substantive reach.

This decision suggests that going forward, prosecutors should expect closer judicial scrutiny and be prepared to return to court more frequently, rather than relying on catchall authorizations.

In light of the fact that such omnibus orders are incredibly helpful tools in ongoing criminal investigations, one should expect prosecutors to continue to seek them, amending their applications pursuant to In Re: Sealed Case. But the takeaway from the other side of the "v." is also clear: Service providers, companies and people will no longer be passive recipients of sealed subpoenas. This case reinforces their role as important gatekeepers of user privacy.

Companies receiving NDOs should be prepared to review whether the order is supported by meaningful judicial findings, not merely by prosecutorial assertion; evaluate whether the subpoena is narrowly tailored and consistent with the underlying order; and, finally, consider challenging NDOs that are overly broad, vague or facially unauthorized.

Moreover, recipients should press prosecutors on a fundamental question: Is the recipient a target or merely a witness? The court drew a crucial distinction here. Disclosure may pose a greater risk in the case of targets, but not necessarily for peripheral witnesses.

Not every company wants to pick a fight for the sake of disagreement or some larger policy. And it would be safe to assume that many individuals and entities likely would want to cooperate with ongoing criminal investigations, but only with offered clarity. Otherwise, the omnibus NDO stands at the crossroads of a possible challenge.

Finally, while the decision doesn't prohibit all prospective NDOs, its skepticism of blanket orders is unmistakable. For government attorneys, this means that convenience and speed are no longer sufficient to sacrifice statutory process.

For companies and their counsel, it provides a potent new argument for transparency and judicial accountability. The broader message is that the judiciary remains a check on executive power, particularly in the growing domain of digital surveillance and compelled silence.

**Conclusion**

The D.C. Circuit's opinion in In re: Sealed Case is more than a procedural correction — it's a reminder that secrecy must be earned, not assumed. Courts, not prosecutors, are the arbiters of when silence is justified under the law. As digital investigations become more complex and intrusive, that principle will only grow more vital.

---

*Gregory P. Rosen is a shareholder at Rogers Joseph O'Donnell PC. He previously served as an assistant U.S. attorney, chief of the Capitol Siege Section, and chief of the Federal Major Crimes Section in the U.S. Attorney's Office for the District of Columbia.*



[1] In re Sealed Case, No. 24-5089 (D.C. Cir. July 18, 2025).

[2] 18 U.S.C. § 2705(b).

[3] 18 U.S.C. § 2705(b).

[4] In Re Sealed Case, 24-5809 (D.C. Cir. July 18, 2025), at *3-4.

[5] Id. at *4.

[6] Id.

[7] Id. at *7-8.

[8] Id. at *8-9.

[9] Id. at *11.

[10] Id. at *8.

[11] Id.