

---

July 28, 2025

# D.C. Circuit Limits Scope of Non-Disclosure Orders Under the Stored Communications Act

On July 18, in *In re Sealed Case*,<sup>1</sup> the U.S. Court of Appeals for the D.C. Circuit invalidated an open-ended non-disclosure order (“NDO”) issued under Section 2705(b) of the Stored Communications Act. NDOs are commonly obtained by U.S. law enforcement to prevent disclosure of legal process seeking information about users of various communications services, such as email providers, particularly when investigators have concerns that a sensitive investigation will be impacted if users learn about the existence of the legal process. Section 2705(b) allows for the issuance of NDOs under circumstances in which certain enumerated harms might result from disclosure.<sup>2</sup> Under the court of appeals’ decision, a court may no longer issue an NDO without making a finding that there is a “reason to believe” that disclosure will result in harms specified in the statute, rather than deferring to the judgment of the government. The court of appeals held that the specific NDO at issue was unlawful because it authorized law enforcement to prohibit disclosure based on the government’s *own* determinations about harms that might result.

Although the court of appeals’ holding appears narrow, it may have significant consequences for law enforcement agencies and companies that routinely receive legal process, such as electronic communication service providers. Moreover, the court of appeals’ skepticism about prospective NDOs that cover subpoenas or warrants not yet issued—sometimes called “omnibus” or “case-wide” NDOs—could foreshadow that some courts will scrutinize such NDOs more closely.

## Background

The Stored Communications Act prohibits disclosure of customer records except in defined circumstances, including where law enforcement complies with certain processes.<sup>3</sup> In general, the procedural requirements and level of proof required to obtain that data grows more stringent under the Act as more intrusive information about the user is sought.<sup>4</sup>

As a default, such a company is permitted to notify a user that it has received legal process concerning their records. But Section 2705(b) allows the government to apply for a court order—an NDO—to prohibit that disclosure.<sup>5</sup> The statute provides that the court “shall enter” an NDO “if it determines that there is reason to believe that notification” will result in various specified consequences:

1. “endangering the life or physical safety of an individual”;

---

<sup>1</sup> 2025 WL 2013687 (D.C. Cir. July 18, 2025).

<sup>2</sup> See 18 U.S.C. § 2705(b).

<sup>3</sup> See *id.* §§ 2702, 2703.

<sup>4</sup> See *id.* § 2703.

<sup>5</sup> See *id.* § 2705(b).

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.”<sup>6</sup>

The scope of Section 2705(b) has rarely been litigated at the appellate level. Before the July 18 decision, the most recent published appellate decision was issued in 2023, when Twitter (now X) unsuccessfully brought a First Amendment challenge to an NDO accompanying a search warrant.<sup>7</sup>

The D.C. Circuit’s July 18 decision concerned another challenge by X to an NDO. This time, however, the company’s objection focused on the open-ended nature of the order in question: a magistrate judge had authorized an NDO for a year that could cover any subpoena the government might issue in a given investigation.<sup>8</sup> In other words, the magistrate judge’s order would have allowed the government to append the general NDO to all future process issued in the case, without further application to the court. Rather than making its own finding that there was a reason to believe that disclosure of all future subpoenas would result in the harms specified in the statute, the magistrate judge ordered the government to determine whether disclosure of the subpoena would result in “potential target(s) attempting to evade apprehension, or destroy or encrypt evidence, or otherwise seriously jeopardizing the investigation.”<sup>9</sup> When X challenged that NDO after receiving a subpoena for user records, the district court upheld the order.<sup>10</sup>

### The D.C. Circuit’s Decision

The D.C. Circuit reversed, explaining that Section 2705(b) required a *court*—not an investigator—to determine that there was reason to believe that one of the specified harms in Section 2705(b) would result from disclosure of the legal process.<sup>11</sup> The court further identified two concerns with the specific NDO at issue: the order (i) applied prospectively and (ii) “provided no meaningful limit on the potential targets of the future subpoenas.”<sup>12</sup> Therefore, even if the magistrate judge issuing the subpoena had tried to find a “reason to believe” that a harm would result from disclosure, the court of appeals doubted that such a finding could be made.<sup>13</sup>

The court of appeals did emphasize that its holding was “narrow.”<sup>14</sup> It stated that it would not “rule out the possibility that, in another case, the government might seek a prospective order with clearer limitations or other features that could allow a court to make the requisite findings.”<sup>15</sup> Although it was skeptical that a future broad, prospective order would be permissible, it considered its holding to be narrow because the magistrate judge did not even purport to make the “requisite findings.”<sup>16</sup> Similarly, the court of appeals accepted that an NDO could apply to multiple subpoenas, so long as the issuing court made a “reason to believe” determination for each of those subpoenas.<sup>17</sup>

### Takeaways

The D.C. Circuit’s decision sets forth rare appellate guidance about the steps that judges and law enforcement agencies must follow when seeking NDOs. Its holding that a court, and not the government, must “make the requisite findings” under Section 2705(b) clarifies that even NDOs covering multiple subpoenas, orders or warrants must be accompanied by commensurate

---

<sup>6</sup> *Id.*

<sup>7</sup> *See In re Sealed Case*, 77 F.4th 815 (D.C. Cir. 2023). In that case, Twitter had also argued that the district court misapplied the requirements of Section 2705(b), but the court of appeals held that Twitter had forfeited that argument. *See id.* at 829.

<sup>8</sup> *See In re Sealed Case*, 2025 WL 2016387, at \*2.

<sup>9</sup> *Id.* (citation omitted).

<sup>10</sup> *Id.*

<sup>11</sup> *Id.* at \*5–6.

<sup>12</sup> *Id.* at \*4–5.

<sup>13</sup> *Id.* at \*5.

<sup>14</sup> *Id.* at \*6.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

## D.C. Circuit Limits Scope of Non-Disclosure Orders Under the Stored Communications Act

---

judicial findings.<sup>18</sup> While the court left open the level of specificity with which a court must articulate those findings—and even suggested that an NDO can cover “categories” of subpoenas rather than only specific subpoenas—it explained that an issuing court must “match its required statutory findings to the breadth and variety of potential subpoenas to which its nondisclosure order could apply.”<sup>19</sup>

The D.C. Circuit’s skepticism about the challenged NDO’s combination of prospectivity and open-endedness also may suggest that some courts will review omnibus NDOs with additional care, particularly when the government seeks a single NDO to address an indeterminate number of subpoenas or similar process. Nonetheless, the court emphasized that its hesitations about these features did not form the basis of its holding. Therefore, the doctrinal impact of the court’s broader concerns about certain omnibus NDOs may wait for future decisions.

---

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* at \*5–6.

\* \* \*

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

**John P. Carlin**

+1-202-223-7372

[jcarlin@paulweiss.com](mailto:jcarlin@paulweiss.com)

**Katherine B. Forrest**

+1-212-373-3195

[kforrest@paulweiss.com](mailto:kforrest@paulweiss.com)

**Anna R. Gressel**

+1-212-373-3388

[agressel@paulweiss.com](mailto:agressel@paulweiss.com)

**Elizabeth Hanft**

+1-212-373-3664

[ehanft@paulweiss.com](mailto:ehanft@paulweiss.com)

**David K. Kessler**

+1-212-373-3614

[dkessler@paulweiss.com](mailto:dkessler@paulweiss.com)

**Peter Carey**

+1-202-223-7485

[pcarey@paulweiss.com](mailto:pcarey@paulweiss.com)

**Justin D. Lerer**

+1-212-373-3766

[jlerer@paulweiss.com](mailto:jlerer@paulweiss.com)

**Audrey M. Paquet**

+1-212-373-2397

[apaquet@paulweiss.com](mailto:apaquet@paulweiss.com)

*Associate Matthew J. Disler contributed to this Client Memorandum.*