ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

JULY 7, 2021

A Practical Guide to Challenging Gag Orders Under the Stored Communications Act

by Kellen Dwyer and Kim Peretti

Nondisclosure orders, also known as "gag orders" or NDOs, are once again in the news following reports that the Justice Department obtained data of reporters and members of Congress from third-party internet service providers and used NDOs to prevent the providers from informing their customers of the government's requests. At the same time, U.S. companies are under increasing pressure from the European Union to push back on NDOs. The European Commission recently approved standard contractual clauses (SCCs) that would require U.S.-based companies that receive data from the EU to notify the transferring entity (the "data exporter" in GDPR-speak) and the data subject of any U.S. government requests for the data. If an NDO prohibits the U.S.-based company from providing such notice, the SCCs would require the company to "use its best efforts to obtain a waiver" from the NDO "with a view to communicating as much information as possible, as soon as possible," and to document such efforts.

Given these developments, companies may wish to consider updating their policies concerning government requests for information, generally, and NDOs, specifically, and challenging them when appropriate.

What Is a Nondisclosure Order?

The Stored Communications Act (SCA) regulates the government's ability to obtain data from companies that constitute an "electronic communication service" or a "remote computing service" within the meaning of the statute. Section 2703 allows the government to issue subpoenas and to obtain search warrants and other legal process for data held by such companies. Section 2705(b) permits courts to issue NDOs that prevent companies from notifying their customers (or anyone else, for that matter) of the existence of legal process issued under Section 2703. To obtain an NDO, the government must convince a magistrate that there is "reason to believe" that notification will result in:

- Danger to life or physical safety.
- Flight from prosecution.
- Destruction of evidence.
- Intimidation of witnesses.
- Serious jeopardy to an investigation or undue delay of a trial.

Section 2705(b) does not explicitly cap the duration of NDOs, stating only that they may be issued for "such period as the court deems appropriate."

Does the Justice Department Have Policies Governing the Use of NDOs?

Yes. In 2017, Deputy Attorney General Rod Rosenstein issued a memorandum limiting the use of NDOs. It requires that prosecutors:

- Conduct an "individualized and meaningful" assessment of the need for an NDO and only seek an NDO when circumstances require.
- Tailor NDO applications to include specific facts that satisfy the particular legal bases specified in Section 2705(b), rather than relying on boilerplate statutory language.
- Refrain from seeking an NDO lasting over one year unless justified by exceptional circumstances. Prosecutors may seek to renew NDOs after one year if the facts continue to support nondisclosure.

Does the Justice Department Have Specific Guidance on Issuing SCA Process to Cloud Service Providers to Obtain Their Enterprise Customers' Data?

Yes. The DOJ's Computer Crime and Intellectual Property Section (CCIPS) issued guidance in 2017 urging prosecutors not to seek enterprise customer data from cloud service providers unless it is necessary. The guidance recognizes that the migration of business emails and other sensitive corporate documents from onsite storage to third-party cloud service providers has created a loophole of sorts under the SCA. It means that the government can now obtain a business's most sensitive information directly from its cloud provider, without the targeted company's knowledge, simply by obtaining legal process and an NDO under the SCA. The CCIPS guidance discourages this practice, stating that "in general, prosecutors should seek data directly from the enterprise, rather than its cloud-storage provider, if doing so will not compromise the investigation." Of course, "[i]f law enforcement has developed reasons to believe that the enterprise will be unwilling to comply [with legal process] or if the enterprise itself is principally devoted to criminal conduct, seeking disclosure directly from the cloud provider may be the only practical option." Otherwise, prosecutors should consider whether there are persons within the enterprise, such as the general counsel, who could be trusted not to alert members of the company who are suspected of wrongdoing. Involving the company's counsel also affords the business "the opportunity to interpose privilege and other objections to disclosure for appropriate resolution." Finally, the guidance asks prosecutors to consider whether any evidence destruction concerns may be mitigated by serving a preservation letter on the cloud provider under Section 2703(f) before notifying members of the company.

Are There First Amendment Limitations on Nondisclosure Orders?

Yes. Courts have almost uniformly held that NDOs trigger strict scrutiny under the First Amendment, because they constitute either a prior restraint or a content-based regulation of speech, or both. In order to satisfy strict scrutiny, the government must demonstrate that the NDO is narrowly tailored to promote a compelling interest and that there are no less restrictive alternatives to achieve the government's purpose. When a plausible, less restrictive alternative is offered, it is the government's obligation to prove that the alternative will be ineffective to achieve its goals.

What Is the Procedure for Challenging NDOs in Court?

Courts have found that providers that receive an NDO have suffered injury in fact sufficient to confer standing. These challenges are typically brought by filing an application in the court that issued the NDO seeking either to alter the NDO or to quash it altogether. The provider's application must demonstrate that the company has been harmed by its inability to notify its customer of the government's request. The burden then shifts to the government to demonstrate that the NDO is the least restrictive means of satisfying its compelling interest in protecting the particular investigation at issue.

While courts typically allow the government to file at least part of its response ex parte, providers have a number of options to ensure they receive enough information to allow for an effective reply. The provider could suggest that the government file a brief setting forth its legal arguments under seal but not ex parte, and then, if necessary, separately file an ex parte affidavit informing the court of any relevant facts that cannot be disclosed to the provider's counsel. The provider could also propose a protective order that would allow the provider's counsel to learn any sensitive information the government relies on in defending the NDO on the condition that such information is for counsel's eyes only.

How Is a Challenge to an NDO Most Likely to Be Successful?

Challenging an NDO issued by a federal judge at the request of the Justice Department is not easy. The recipients of such orders often have little information with which to question the magistrate's finding that there is reason to believe that disclosure will compromise a criminal investigation. The provider does not receive a copy of the government's application for the NDO. Rather, it only receives the NDO itself, which typically just parrots the language of Section 2705(b) and says nothing about the nature of the investigation or how exactly it could be compromised by notification. Apple illustrated the dilemma faced by many providers in response to recent revelations that it complied with a subpoena and NDO concerning data of congressional staff members. Apple explained publicly that, because the subpoena and NDO provided no information on the nature of the investigation, it would have been virtually impossible for Apple to understand the intent of the desired information in order to object to the process or dispute the court's findings. Moreover, major technology companies receive thousands of data requests from law enforcement every week, making it difficult to meaningfully review, much less challenge, every NDO. Still, there are some red flags that can be gleaned from the NDO itself, from the accompanying legal process or from the provider's own records that might indicate that an NDO is ripe for challenge. Moreover, bringing a challenge itself may allow the provider's counsel to learn more information to better test the government's need for secrecy.

1. The NDO exceeds one year in duration

Several courts have held that NDOs of indefinite duration violate the First Amendment. This is a straightforward application of strict scrutiny: since the government's need for secrecy will always expire at some point, an indefinite ban will never be narrowly tailored. Similarly, setting an expiration date, with the possibility of an extension upon a showing of continued need, will always constitute a less restrictive means than an indefinite NDO.

Whether a court would uphold NDOs that last for a definite period of over a year is less clear. DOJ policy prohibits such NDOs, absent extraordinary circumstances, and several courts have suggested that 180 days might be a better default period. Despite this guidance, it is not uncommon for courts to grant two-year NDOs, particularly in categories of cases that are considered especially sensitive, such as those relating to national security. But the subject matter of an investigation says very little about the length of time secrecy will be needed in any particular case. A company that receives an NDO lasting for more than a year should consider challenging the government to justify why the extended period is necessary in the particular case.

2. *The NDO relates to an enterprise customer and does not permit disclosure to the enterprise's legal counsel and top executives*

As noted, Justice Department policy counsels against seeking data from an enterprise's cloud service provider, unless there is reason to believe the enterprise is "principally devoted to criminal conduct" or otherwise "unwilling to comply" with legal process. Providers should consider challenging any NDO that prohibits notification to an enterprise customer (unless they agree that the enterprise is principally devoted to crime, in which case they should consider terminating the service contract!). To be sure, DOJ guidance is not legally binding, and in some cases, the government may have legitimate reasons to fear that notification to an enterprise risks compromising the investigation. Still, it may be worth challenging the government to meet its burden to show why there is not a single person in the enterprise who could be trusted with notification. As part of this challenge, a company may consider proposing the less restrictive means suggested by the CCIPS guidance, including serving preservation requests on the cloud provider before notifying the enterprise and limiting notice to particular trusted persons in the enterprise.

3. *The NDO relates to a public investigation*

It is not uncommon for NDOs to relate to investigations that are already public. This may occur when the government has already indicted the target of the request or a related person, or otherwise officially confirmed the investigation, or where the existence of the investigation has been reported in the press. While NDOs themselves rarely identify the nature of the investigation, some information may be gleaned from the accompanying subpoena, search warrant, or 2703(d) order. Providers should consider conducting basic research to determine whether an NDO appears to relate to an investigation that is already public. If it does, this may be a basis to challenge the government to explain why there is nonetheless still a compelling need for secrecy.

4. *The company is not subject to the SCA*

The SCA only applies to companies that constitute an electronic communication service (ECS) or a remote computing service (RCS) under the statute. An ECS is "any service which provides to users thereof the ability to send or receive … electronic communications." A "remote computing service" includes "the provision to the public of computer storage or processing services by means of an electronic communications system." As more and more companies provide their customers with internet access or the ability to communicate over the company's app, the reach of the SCA grows ever larger. Indeed, the government has argued (successfully in some cases) that the SCA applies not only to companies whose primary business involves provision of internet services but to any company that provides their customers with internet access or a chat function. Companies that are not primarily and obviously engaged in providing electronic communication or storage to the public should consider whether to challenge process under the SCA, including NDOs, on the ground that the company is not covered by the statute.

Is There a Benefit to Negotiating the Terms of an NDO with the Government?

Yes. Prosecutors frequently agree to alter NDOs, as well as the underlying legal process, in response to a provider's concerns. Most prosecutors want to maintain good relations with providers, with whom they must frequently deal, and are eager to avoid the legal risk and resource expenditure inherent in litigation. Cautious by nature, it is not uncommon for prosecutors to seek a broad NDO initially, but then agree to reasonable modifications when approached by the provider's counsel. This appears to be what happened when Google received an NDO barring it from informing *The New York Times* of a request for data related to four *Times* reporters. According to the *Times*, Google successfully convinced prosecutors to revise the NDO to allow it to inform an attorney for the *Times* who, in turn, convinced the

prosecutor to further revise the NDO to permit him to notify additional attorneys and two of the newspaper's top executives. The NDO was eventually dropped entirely.

How Should Companies Guard Against NDOs Going Forward?

There are a number of steps that companies can take to protect themselves and their customers from NDOs.

- Companies (in particular providers subject to the SCA) could consider implementing a policy that challenges government requests and NDOs, in particular, in certain specified circumstances or whenever there is a lawful basis to do so. Microsoft, for instance, has committed to challenging "every government request for public sector or enterprise customer data—from any government—where there is a lawful basis for doing so." Companies could also include as part of the policy that they will challenge any NDO over a certain length of time or that relates to particularly sensitive accounts. Such policies may deter government overreach—prosecutors are well aware of each company's legal process policies (if published) and are less likely to push the envelope if they expect pushback. In addition, any policy showing a commitment to data protection could help a company comply with the GDPR and its data transfer provisions.
- Companies (in particular providers subject to the SCA) could also consider formalizing a policy of disclosing government data requests to their customers whenever they are legally permitted to do so. In addition to demonstrating a commitment to privacy, these policies can help a company establish standing to challenge an NDO.
- Companies could further consider including a provision in relevant customer contracts with providers to provide notice to customers of government requests for their data. While contractual agreements obviously cannot trump a lawful court order, they can provide a more specific basis to challenge an NDO, both in negotiations with prosecutors and, if necessary, in litigation. Indeed, lawyers for Google and The *New York Times* credited a contractual provision requiring Google to inform the *Times* of government data requests for its successful challenge to a recent NDO. Similarly, the SCCs recently approved by the European Commission require data importers to inform data subjects and data exporters of all requests for data transferred under the SCCs and to challenge any NDO that would prevent such notice. In addition to complying with the GDPR, such contractual clauses can help providers fight back against expansive NDOs.

You can subscribe to future *Privacy, Cyber & Data Strategy* advisories and other Alston & Bird publications by completing our **publications subscription form**.

Learn more about our **Privacy, Cyber & Data Strategy Team**.

Learn more about our **National Security & Digital Crimes Team**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Co-leaders of the National Security & Digital Crimes Team

Kellen Dwyer
202.239.3240
kellen.dwyer@alston.com

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333