Last year, University of California, Berkeley became the first university to release a transparency report of all non-consensual electronic data requests made by government officials. Privacy advocates lauded the release as a bold move toward greater transparency, although a few statistics were missing from the report. Transparency reports of electronic data requests are common for major communications and technology companies, but universities, which often act as small internet service providers, have yet to embrace transparency. Security activists are calling on universities to develop their own transparency reports, but it is important to understand what information these reports are not reporting. Berkeley's transparency report excluded subpoenas with gag orders, the now infamous FISA court requests, and one of the more furtive methods of government surveillance, National Security Letters (NSLs).

In December 2015, Nicholas Merrill won an eleven-year legal battle over a single NSL. In 2004, the FBI issued the NSL to Merrill, the owner of Calyx Internet Access, requesting information on a customer. Like almost all NSLs, the request included an indefinite gag order. Merrill filed suit against the request in 2004 and engaged in a series of appeals for over a decade. In 2010, Merrill was able to reveal his identity in the case and last December, the court ruled Merrill could release the un-redacted NSL request, finally shedding light on the exact nature of the letter sent to Merrill.

The FBI began issuing NSLs in 1986, following an amendment to the Right to Financial Privacy Act, which permitted NSLs to obtain financial records for foreign counterintelligence matters. The FBI's authority was expanded by Section 505 of the PATRIOT Act in 2001. Now, NSLs provide a means of requesting information without authority from a court or suspicions of anyone associated with the individual under investigation. The number of NSL requests rose from fewer than 9,000 in 2000 to 39,000 in 2003, approximately. The FBI is required to provide Congress with a semiannual account of NSL requests, reporting 400,000 requests between 2003 and 2011, according to the DOJ Inspector General's 2014 report. The Inspector General's report also noted that the percentage of US citizens investigated through NSLs steadily rose from 39% in 2003 to 63% in 2009.

NSL requests are officially restricted to non-content information. The scope of acceptable requests includes "transactional information" like merchandise orders, phone numbers, IP addresses, and screen names connected with an account. NSLs can request email addresses

"associated" with the individual under investigation's email accounts, which includes anyone who has sent emails to or received emails from the individual. While the content of emails is not available, an individual's network is fair game. At the same time, the official restrictions placed on NSL requests do not always align with the practice of issuing requests.

The Merrill case provided a glimpse at the disparity between sanctioned and requested information. In the recently released NSL request attachment, the FBI asked Merrill to provide web history, IP addresses of anyone in contact with the individual, and a radius log, which Merrill believes implied cell phone positioning. The final request was for "any other information which [Merrill] considers to be an electronic communication transactional record."

The oblique wording could certainly cause confusion about what records the FBI is requesting. The 2014 Office of the Inspector General (OIG) sample review found 19 out of 165 NSLs returned data not sanctioned by NSL statutes. In 17 of the 19 cases, the FBI did not attempt to remedy the unlawful information. The OIG suggested that even agents themselves might not have been aware of what types of data they could collect.

Several incidents in recent years typify the potential overreach allowed through NSL requests. First, the DOJ Inspector General reported an incident of the FBI using an NSL request to gather data after a court denied a subpoena for the same information. Second, the FBI used NSLs to gather data on reporters for the *New York Times* and the *Washington Post*.

Target and data overreach are not the only potential threats of NSL usage. In the first few years following the PATRIOT Act's passage, hasty execution led to rampant errors in NSL procedures, reporting, and appropriate use. The 2014 OIG report states that many errors have been mitigated with the development of a subsystem for handling NSL requests, but the report still found filing errors in 52% of the NSL cases sampled, including 28 missing NSLs.

Given the opaque nature of NSL requests, it is difficult to determine whether requests are even effective. OIG cited examples of NSL requests providing relevant information to FBI cases in the second NSL report. However, OIG did not compare the effectiveness of NSL requests over measures with more transparent information request methods like subpoenas. Without more transparency, the use of NSL requests amounts to an investigative shortcut at the cost of civilian privacy.

In early 2014, technology and communications companies successfully lobbied for permission to publicly report the number of NSL requests, although they are limited to only providing a range of requests, not specific numbers. The range, typically reported as 0-999, obfuscates an exact understanding of the extent. Google stated that NSL and FISA requests, warrants issued by a special court to investigate foreign entities within the country, increased 250% between 2009 and 2014. Given that FISA requests are usually single requests for thousands of individuals, the rise explicates the increase of NSL requests.

In 2015, the USA Freedom Act was passed a day after the PATRIOT Act expired. The Act notably requires the FISA court to make public any significant cases, which could potentially provide more transparency to the notoriously hidden surveillance mechanism. National Security Letters received less reform: Congress revised the guidelines for NSLs so the gag order would expire three years after issuance or at the conclusion of an investigation, but this change still firmly places control of the release of information in the issuer's hands.

The number of surveillance tools in the hands of government agencies does not appear to be shrinking. All OIG reports indicate that the FBI now views NSLs as a "crucial" tool for investigation. With each new allowance, the public must understand that going forward means rarely going back. The OIG reports note only a single period of decreased NSL use between 2007 and 2009, which agents explained as a reaction to an increased scrutiny of the agency's use of NSLs. Consistent inspection of these covert methods is the only way to prevent misapplication, but the public cannot monitor what it does not see.

UC Berkeley's transparency report should be commended, but only as a step in the right direction. In some sense, the transparency report inaccurately represents the prevalence of government inquiry; one of the most utilized tools is not legally reportable. Berkeley's transparency notes there is missing data, but is unable to explain the extent of that data. Current transparency reports are essentially not transparent. Universities that decide to disclose similar reports need to actively combat the illusion of transparency such reports create.

---

**Harrison Speck**

Harrison is a former Senior Content Editor for the Cornell Policy Review and 2017 CIPA graduate focused on tech policy. During his time at Cornell, he was a Google Public Policy fellow with the Future of Music Coalition. Before Cornell, he worked for the State of Texas in public assistance eligibility and child welfare with Texas Department of Family and Protective Services. He is an avid musician and technology enthusiast.
View all posts