Young and old alike, Facebook is where millions of people around the world share details of their lives that might have gone unshared 13 years ago. And if the recently released Facebook report on government requests for this data is any indication, law enforcement agencies within the United States are very interested in what the public is doing.

The biannual look at the nuts and bolts of these requests, published by the social media company April 27, tells us that authorities are more aware than ever of the value that social media data holds.

In the four years the company has been compiling the post-request report, both the numbers of requests and the number of individual accounts targeted have risen in tandem throughout the U.S.

FB LE Data Requests (Part 1)

The broad disclosures are published after what the social media called a careful review of each request and compliance with laws and terms of service.
According to the social media giant, roughly 56 percent of requests made in the U.S. are accompanied by a non-disclosure order, which bars the company from notifying affected users.

Between July and December 2016, the company received:

- 14,736 search warrant requests;
- 6,536 subpoenas;
- 738 court orders (18 USC 2703(d));
- 236 court orders (non-18 USC 2703(d));
- 1,948 pen register/trap and trace requests;
- 1,695 emergency disclosures; and
- 125 real-time wiretap requests.

As one might expect from an increase in overall requests for data, the percentage of produced data on the part of Facebook has also increased slightly — hovering just around the 80 percentile mark for the last four years.

**FB Report - Requests Granted 2013-2016**

Worldwide, the company reports an increase in user data requests of 9 percent.

From the viewpoint of the American Civil Liberties Union (ACLU), the disclosures are an essential part of transparency in legal process that stands badly out of date.

Nicole Ozer, technology and civil liberties policy director for the ACLU of California, said where California law has seen updates, federal communications privacy law remains a point of serious concern, as it has not been updated in the last 31 years.

“The federal law, the Electronic Communications Privacy Act, is supposed to … make sure there are proper safeguards in place for when the government can demand electronic information, including things like data from Facebook,” she said. “That law has not been updated since 1986. In 1986, cellphones were the size of bricks, Mark Zuckerberg was still in diapers, the World Wide Web did not even exist.”

As a result of the gaps in the federal law, Ozer said law enforcement agencies across the country have pursued various forms of digital communications more aggressively, and without some of the checks and balances required of other investigative avenues.

She boils the issue down to three major categories:

1. Information sought by police that exists in the open;
2. Information collected through third-party sources — like the controversial partnership between Geofeedia and various law enforcement agencies; and
3. Information that exists on the back end of platforms and services that isn’t readily visible to the public.

In the case of Geofeedia, the company was compiling intelligence data collected through social platforms for use by police and other law enforcement. Since the revelations, both Twitter and Facebook have cut ties with the third-party.
The latter category is where Ozer sees the most risk of overreach.

“This data isn’t publicly available where you can just go onto Facebook; this is actually data held by the back end of the company and you are compelling it with a warrant or another type of legal process,” she said. “That third piece, the kind of legal process that is required for sort of accessing this very sensitive back-end data, that law has not been updated and it leaves a lot of gray areas, which can make users quite vulnerable.”

And in this increasingly connected world, Ozer said she only expects the interest in user data to increase on the part of law enforcement. Though California was able to solidify its own rules around digital privacy, efforts at the federal level have not resulted in new protections just yet despite bipartisan support.

Though the Electronic Frontiers Foundation (EFF), an organization dedicated to issues of online privacy and law, could not be reached for an interview, a spokesperson said told Government Technology via email that as a general matter, “we’ve seen a consistent increase in the number of user data requests by the government, so the increase at Facebook is part of a general trend.”

Facebook and the U.S. Department of Justice could not be reached for comment as of press time Wednesday afternoon.

http://www.govtech.com/social/Law-Enforcement-Agencies-Requests-for-Facebook-Data-Continue-to-Rise.html