APPLE'S TRANSPARENCY NUMBERS SUGGEST CLAIMS OF GOING DARK OVERBLOWN

Apple recently released its latest transparency report for the period ending June 30, 2015. By comparing the numbers for two categories with previous reports (2H 2013, 1H 2014, 2H 2014) we can get some sense of how badly Apple's move to encrypt data has really thwarted law enforcement.

Thus far, the numbers show that "going dark" may be a problem, but nowhere near as big of one as, say, NY's DA Cy Vance claims.

The easier numbers to understand are the national security orders, presented in the mandated bands.

	NatSec Orders Received	Accounts Affected
1/1/15-6/30/15	750-999	250-499
7/1/14-12/31/14	250-499	0-249
1/1/14-6/30/14	0-249	0-249
7/1/13-12/31/13	0-249	0-249

Since the iPhone 6 was introduced in September 2014, the numbers for orders received have gone up — one band in the second half of 2014, and two more bands in the first half of this year. Curiously, the number of accounts affected haven't gone up that much, possibly only tens or a hundred more accounts. And Apple still gets nowhere near the magnitude of requests Yahoo does, which number over 42,000.

Equally curiously, in the last period, Apple clearly received more NatSec orders than accounts affected, which is the reverse of what other companies show (before Apple had appeared close to one-to-one). One thing that might explain this is the quarterly renewal of Pen Register orders for metadata of US persons (which might be counted as 4 requests for each account affected).

In other words, clearly NatSec requests have gone up, proportionally significantly, though Apple remains a tiny target for NatSec requests compared to the bigger PRISM participants.

The law enforcement account requests are harder to understand.

	# LE Account Requests	# Accounts Specified	# for which Data Disclosed	# Where Apple Objected	# Where No Data Disclosed	# Where Non-Content Disclosed	# Where Content Disclosed	Percent Where Some Data Disclosed
1/1/15-6/30/15	971	2727	1407	116	181	495	295	81%
7/1/14-12/31/14	788	5267	4662	75	155	445	188	80%
1/1/14-6/30/14	789	1739	928	86	185	449	155	77%
7/1/13-12/31/13	638	1380	795	68	182	355	101	71%

Note, Apple distinguishes between device requests, which are often users seeking help with a stolen iPhone, and account requests, which are requests for either metadata or content associated with an account (and could even include purchase records). The latter are the ones that represent law enforcement trying to get data to investigate a user, and that what I've laid out the latter data here [note, I fully expect to have made some data errors here, and apologize in advance — please let me know what you see!!].

Here, too, Apple has seen a significant increase, of 23%, over the requests it got in the second half of last year. Though, note, the iPhone 6 introduction would not be the only thing that would affect this: so would, probably, the June 2014 Riley Supreme Court decision, which required law enforcement to get a warrant to access cell phones, would also lead law enforcement to ask Apple for data more often.

Interestingly, however, there were fewer accounts implicated in the requests in the last half of the year, suggesting that for some reason law enforcement was submitting requests with a slew of accounts listed for each request. Whereas last year, LE submitted an average of over 6.5 accounts per request, this year they

have submitted fewer than 3 accounts per request. This may reflect LE was submitting more identifiers from the same account — who knows?

The percentage of requests where content was obtained has gone up too, from 16% in 2013 to 24% in the first period including the iPhone 6 to 30% last quarter. Indeed, over half the period-on-period increase this period may stem from an increase in content requests (that is, the 107 more requests where content was obtained in the first half of the year, which was a period in which Apple got 183 more requests overall). Still, that number, 107 more successful requests for content this year than the second half of last year, seems totally disproportionate to NYC DA Cy Vance's claim that the NYPD was unable to access the content in 74 iPhones since the iPhone 6 was established (though note, that might represent 1 request for content from 74 iPhones).

Perhaps the most interesting numbers to compare are the number of times Apple objected (because the agency didn't have the right kind of legal process or a signed document) and the number of times Apple disclosed no data (which would include all those times Apple successfully objected — which appears to include all those in the first number — as well as those times Apple didn't have the account, as well as times Apple was unable to hand over the data because a user hadn't used default iCloud storage for messages. [Update, to put this more simply, the way to find the possible number of requests where encryption prevented Apple from sharing information is to subtract the Apple objected number from the no data number.] In the second half of 2013, Apple did not disclose any data 28.5% of the time. In the first half of this year, Apple did not disclose any data in just 18.6% of requests. Again, there are a lot of reasons why Apple would not turn over any data at all. But in general, cops are getting data more of the time when they give Apple requests than they were a few years ago.

More importantly, for just 65 cases in the first half of this year and 80 cases in the second half of last year did Apple not turn over any data for a request for reasons other than some kind of legal objection — and those numbers are both lower than the two half years preceding them. Each of those requests might represent hundreds of phones, but overall it's a tiny number. So tiny it's tough to understand where the NYPD's 74 locked iPhones (unless they did request data and Apple actually had it).

There's one more place where unavailable encrypted data might show up in these numbers: in the number of specific accounts for which data was disclosed. But as a percentage, what happened this year is not that different from what happened in 2013. In the second half of 2013, Apple provided some data (and this can be content or metadata) for 57.6% of the accounts specified in requests. In the first half of this year, Apple provided some data for 51.6% of the accounts specified in requests — not that huge a difference. And of course, the second half of last year, which may be an outlier, but during much of which the iPhone 6 was out, Apple provided data for 88.5% of the accounts for which LE asked for data.

Overall, it's very hard to see where the FBI and other law enforcement agencies are going dark — though they are having to ask Apple for content more often (which I consider a good thing).

Update: In talking to EFF's Nate Cardozo about Apple's most recent report, we agreed that Apple's new category for Emergency Requests may be one other place where iPhone data is handed over (it doesn't exist in the reports for previous half year periods). Apple defines emergency content this way:

> Table 3 shows all the emergency and/or exigent requests that we have received globally. Pursuant to 18 U.S.C. §§ 2702(b)(8) and 2702(c)(4) Apple may voluntarily disclose information, including contents of communications and

> customer records, to a federal, state, or local governmental entity if Apple believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay. The number of emergency requests that Apple deemed to be exigent and responded to is detailed in Table 3.

Given the scale of Apple's other requests, though not in the scale of cloud requests comparatively, these are significant numbers, especially for the US (107) and UK (98).

Of significant note, Apple may give out content under emergency requests.

This is more likely to be a post-Riley response than an encryption response, but still notable given the number.