ABOUT APPLE'S DEAD WARRANT CANARY

There were two significant pieces of Apple security news yesterday.

In laudable news, Apple's new privacy policy makes clear that it will be unable to unlock locally stored content for law enforcement.

> On devices running iOS 8, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access this data. So it's not technically feasible for us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8.

I find the comment as interesting for the list of things Apple envisions potentially having to hand over as I do for the security claim (though the security claim is admirable).

- Photos
- Messages, including attachments
- Email
- Contacts
- Call history
- iTunes content
- Notes
- Reminders

Though Apple's promise to protect this kind of data only goes so far; as the NYT makes clear, that doesn't extend to data stored on Apple's cloud.

> The new security in iOS 8 protects information stored on the device itself, but not data stored on Apple's cloud service. So Apple will still be able to hand over some customer information stored on iCloud in response to government requests.

Which brings us to the second piece of news. As GigaOm notes, Apple's warrant canary indicating that it has never received a Section 215 order has disappeared.

> When Apple published its first Transparency Report on government activity in late 2013, the document contained an important footnote that stated:
>
> "Apple has never received an order under Section 215 of the USA Patriot Act. We would expect to challenge such an order if served on us."
>
> Writer and cyber-activist Cory Doctorow at the time recognized that language as a so-called "warrant canary," which Apple was using to thwart the secrecy imposed by the Patriot Act.
>
> Warrant canaries are a tool used by companies and publishers to signify to their users that, so far, they have not been subject to a given type of law enforcement request such as a secret subpoena. If the canary disappears, then it is likely the situation has changed – and the company *has* been subject to such request.
>
> Now, Apple's warrant canary has disappeared. A review of the company's last two Transparency Reports, covering the second half of 2013 and the first six months of 2014, shows that the "canary" language is no longer there.

Note, GigaOm goes on to mistakenly state that Section 215 is the basis for PRISM, which doesn't detract from the importance of noting the dead warrant canary. The original PRISM slides indicate that Apple started complying with Section 702 (PRISM) in October 2012, and the ranges in Apple's government request data probably reflect at least some of its Section 702 compliance to provide content.

So Apple receiving its first Section 215 order sometime last year would reflect either a different kind of request — one not available by targeting someone overseas, as required under Section 702 — or a request for the kind of information it has already provided via a new authority, Section 215.

Many of the things listed above — at a minimum, call history, but potentially things like contacts and the titles of iTunes content (remember, James Cole has confirmed the government could use Section 215 to get URL searches, and we know they get purchase records) — can be obtained under Section 215.

I find Apple's dead warrant canary of particular interest given the revelation in the recent DOJ IG Report on National Security Letters that some "Internet companies" started refusing NSLs for certain kinds of content starting in 2009; that collection has moved to Section 215 authority, and it now constitutes a majority of the 200-some Section 215 orders a year.

> The decision of these [redacted] Internet companies to discontinue producing electronic communication transactional records in response to NSLs followed public release of a legal opinion issued by the Department's Office of Legal Counsel (OLC) regarding the application of ECPA Section 2709 to various types of information. The FBI General Counsel sought guidance from the OLC on, among other things, whether the four types of information listed in subsection (b) of Section 2709 — the

> subscriber's name, address, length of service, and local and long distance toll billing records — are exhaustive or merely illustrative of the information that the FBI may request in an NSL. In a November 2008 opinion, the OLC concluded that the records identified in Section 2709(b) constitute the exclusive list of records that may be obtained through an ECPA NSL.
>
> Although the OLC opinion did not focus on electronic communication transaction records specifically, according to the FBI, [redacted] took a legal position based on the opinion that if the records identified in Section 2709(b) constitute the exclusive list of records that may be obtained through an ECPA NSL, then the FBI does not have the authority to compel the production of electronic communication transactional records because that term does not appear in subsection (b).
>
> [snip]
>
> We asked whether the disagreement and uncertainty over electronic communication transactional records has negatively affected national security investigations. An Assistant General Counsel in NSLB told us that the additional time it takes to obtain transactional records through a Section 215 application slows down national security investigations, all of which he said are time-sensitive. He said that an investigative subject can cease activities or move out of the country within the time-frame now necessary to obtain a FISA order. [my emphasis]

These Internet company refusals must pertain to somewhat exotic requests, otherwise the government would simply take the companies to court one time apiece and win that authority. So

we should assume the government was making somewhat audacious requests using NSLs, some companies refused, and it now uses Section 215 to do the collection. Another signal that these requests are fairly audacious is that the FISA Court appears to have imposed minimization procedures, which for individualized content must reflect a good deal of irrelevant content that would be suppressed.

While my wildarse guess is that this production pertains to URL searches, everything cloud providers like Apple store arguably falls under the Third Party doctrine and may be obtained using Section 215.

That's not to say Apple's dead canary pertains to this kind of refusal. But it ought to raise new questions about how the government has been using Section 215.

This production will likely be increasingly obtained using USA Freedom Act's emergency provisions, which permit the government to retain data even if it is not legal, if the bill passes. And the bill's "transparency" provisions hide how many Americans would be affected.