RESPONSE TO SNOOPER'S CHARTER: URL SEARCHES ARE BROADLY AVAILABLE IN THE US

In an unsuccessful effort to beat ACLU in a lawsuit over the constitutionality of the Child Online Protection Act, in 2005 DOJ sent a subpoena to Google asking for "all URL's that are available to be located to a query on your company's search engine as of July 31, 2005" and "all queries that have been entered on your company's search engine between June 1, 2005 and July 31, 2005." By challenging the order, Google was able to get the request significantly reduced. But it is understood that DOJ sent the same request to Yahoo, Microsoft, and AOL, and those providers substantially complied (it's possible they negotiated what DOJ claimed was a more reasonable production of 1 million randomly-selected URLs and one week of actual searches with Personally Identifiable Information removed, but they are presumed to have done at least that much).

That's a demonstration of the fact that the Federal government can and has gotten massive amounts of URL data from search engine operators with only a subpoena. The government can and does get such information in criminal investigations with a subpoena as well. The government probably faces more scrutiny when using FISA to get such information, as since 2009 it has likely falled under Section 215 and the minimization procedures finally adopted in 2013, but that would still represent access to URLs with a relevance standard.

Which means the primary limit on the government's access to URL searches with a subpoena in the US is providers' data retention policy. And that means URL searches are, in

general, readily available. Neither Google nor Microsoft state in their privacy policy how long they retain this stuff — though in response to European pressure and to stave off regulation on the issue, in 2010 Google stated it would "only" retain and associate URLs with individual users for 18-24 months, and Microsoft claimed it would only associate Bing records with IPs for 6 months (though that claim is no longer available on its site). Yahoo keeps search data tracked to user for 18 months, with some law enforcement exceptions. All would keep the searches, but de-identify from individual users, thereafter.

Google now permits users to delete past searches (though again, it keeps the searches themselves).

That means for 97% of US users, URL searches will be available to law enforcement with a subpoena for at least 6 months and more often 18 months, unless opting out in Google makes such things genuinely unavailable to law enforcement requests.

On the ISP side, Comcast — which serves half of America's broadband users — in the recent past has said it keeps IP records for 6 months (though I'm not sure if that's still in their privacy policy). Time Warner, which has a 13% market share, doesn't appear to say, though it has said 6 months in the past. So for the overwhelming majority of broadband subscribers in the US, that information will be available for at least 6 months and possibly far longer. That information, too, is available with a subpoena.

I raise this because one of the things in the British Snooper's Charter — a scary, comprehensive new surveillance bill designed, for the most part, to provide legal basis for the existing practice — rolled out earlier this week that people have reacted against is the proposed mandate in the bill that would require all providers to keep records of internet activity for a year. That is a problem. But not only does the proposal appear to be intended for

more targeted use (that is, data retention requests that would override all of the above retention deadlines), it also is explicitly intended for more limited use. Unlike in the US, investigators are not supposed to be able to find out details of what people were doing online. Such information commonly appears in terrorist (especially) criminal cases.

That is, in most areas (not all; location data is one area where UK practice is clearly worse) where the Snooper's Charter seems extreme, the reality for the overwhelming majority of Americans rivals what will be mandated under the UK bill. What the UK bill may do is eliminate the safety of services like DuckDuckGo (which doesn't keep records of your searches), as well as the value of opt-out policies to the extent they really protect a user from law enforcement.

But if people think what's in the Snooper's Charter is bad, then you also need to be worried about the reality in the US for most users.

I will have far more to say about the Snooper's Charter going forward. But one reason why people seem more worried about the Snooper's Charter than similar permissions here in the US is that we have not had a Snowden for the FBI. That is, much of what is described in the Snooper's Charter involves domestic intelligence. And the FBI has never been asked to provide a comprehensive view of all the kinds of surveillance it uses (indeed, it has succeeded in evading legal oversight in a number of ways), and very very little of it got included in Snowden's leaks.

For all the problems of the policies laid out in the Snooper's Charter, at least the UK's spooks and cops have had to reveal what they're actually doing. It's high time for FBI (and DEA and all the other surveillance-crazy domestic law enforcement agencies in the US) to do the same.

Updated: Corrected an error in DOJ's "reasonable" request to Google and tweaked for

clarity.