Friend and colleague Robert Gezelter, CDP points to serious deficiencies in the thinking behind legislation currently under consideration in the House and Senate of the Congress of the United States. The remaining text is entirely Bob’s with minor edits.

* * *

This past February 13, Senator John Cornyn (R-TX) introduced S.436, the “Internet Stopping Adults Facilitating the Exploitation of Today’s Youth Act of 2009” (referred to as the “Internet SAFETY Act”). Representative Lamar Smith (R-TX) introduced a parallel resolution in the House of Representatives, H.R.1076.

Both measures amend 18 USC §2703 <http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002703----000-.html> to require that “A provider of an electronic communications service or remote computing service shall retain for a period of at least two years all records or other information pertaining to the identity of a temporarily assigned network address the service assigns to that user.”

Taken broadly, as some legal commentators have concluded,<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860> such requirements extend beyond the level of commercial Internet Service Providers (ISPs) and ensnare everyone who operates a Wi-Fi hot-spot or firewall, requiring every home or small business to become a long term custodian of network logging data.

This requirement has problems of technical feasibility and accuracy. It may create both a surveillance hazard and subpoena target.

The proposed legislation presumes the use of a network protocol suite that uses hardware MAC addresses, such as the IP suite. and there are serious technical issues. Dynamic addresses are typically managed using the Dynamic Host Configuration Protocol (DHCP), <http://www.ietf.org/rfc/rfc2131.txt>. However, IP address assignment can also be done dynamically without any centralized authority under Microsoft’s “Automatic IP Addressing” (AIPA) <http://www.ietf.org/rfc/rfc3927.txt>. DHCP servers issue “Leases” to requesting machines on a specific IP addresses for a specified period of time, subject to renewal.

The association managed by either scheme depends on associating an IP address with an IEEE 802.3 media access control (MAC) address<http://standards.ieee.org/getieee802/802.3.html>. Although all IEEE 802.3 interfaces have a default hardware MAC address, the default is not always used by software. MAC addresses were never intended as non-forgeable machine serial numbers, and indeed MAC address spoofing (forging) and related attacks are well known security hazards.<http://en.wikipedia.org/wiki/Arp_spoofing> MAC addresses are not a non-repudiable identifier.
Thus, it is quite possible to assume a DHCP lease without any knowledge of the original lessor. When the original lessor is seen to cease operation, the pretender merely assumes the mantle of the original MAC address and continues to use the network.

A second, far more serious problem is time correlation. Log records are reliable only if the timeline recorded in different logs can be correlated to a common clock. Tracking an Internet connection to a given address on one side of a firewall is useful only if it can be determined precisely which address on the far side of the firewall corresponded to that connection (in IP, the port number) at that precise time. Thus, TCP port 8465 may point to one address at 12:00:15 and to a different address at 12:00:30. Absent precisely correlated logs, which connection is the one of interest is not easily determined.

Thus, the attributability of the resulting logs is called into question, even without raising a question of MAC forgery.

There are millions of home and small office firewalls presently deployed. These appliances are not even physically capable of storing the information required without replacement. Who will cover the cost and effort required to upgrade or replace this equipment? Who will incur the cost of preserving the logs generated by this equipment?

There is far more at risk from this legislation than the child pornography referred to in its title and preamble. Bruce Schneier’s comment in a January 29, 2009 essay concerning the Mumbai terror attack is apropos:

“Society survives all of this because the good uses of infrastructure far outweigh the bad uses, even though the good uses are – by and large – small and pedestrian and the bad uses are rare and spectacular. And while terrorism turns society’s very infrastructure against itself, we only harm ourselves by dismantling that infrastructure in response – just as we would if we banned cars because bank robbers used them too.”

Imposing a duty to log all Internet activity on every home and small business, and requiring the data to be retained for two years imposes an unprecedented burden with limited utility. It also poses severe risks for invasions of privacy engendered by this very log data.

A more extensive discussion of this legislation is onlined in “Will Long Term Dynamic Address Allocation Record Retention Help or Hurt?”

[MK adds: You might want to start contacting your Senators and your Representative about this issue.]

***


***