

## The New Real ID for the Internet

January 25, 2011 - The Real ID act was one of the worst pieces of legislation ever passed in this country. The idea behind it was to prevent people from getting a driver's license so that another 9/11 couldn't happen. At least that was the story told to the American people. There is only one problem with that story. Virtually everyone who is familiar with the law and who has looked at the ID's carried by the 9/11 terrorists agrees that if Real ID had been in place at the time, it wouldn't have prevented what happened. Now James Sensenbrenner (R-WI), the same person who crafted Real ID, is exploring new legislation that would allow the government to track everything you do on the internet. Call it "Internet ID". What could possibly go wrong with a law like this?!

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

What Sensenbrenner is proposing sounds simple enough. He wants Internet service providers (ISPs) to store your usage data for up to two years. He's thinking that this information will be helpful for federal investigations into child pornography. That sounds just fine but it's unlikely that this type of data collection would be limited solely to that purpose. The federal government has a real problem with mission-creep in anything it does. So while this data collection might start out with a focus on child pornography, it would inevitably be available for IRS investigations, file sharing investigations and even general snooping on the lives of private citizens. And if that doesn't scare you, then you should also consider that the federal government's record on data security is not exactly exemplary.

If such a law was passed, the data collected wouldn't just be useful to the government. There are a wide variety of private interests that would like access to it too. Advertisers, divorce attorneys, private investigators—all of whom could potentially use this stored information to their advantage. All of that data would be available with a subpoena. And for those more enterprising - like scam artists and hackers - who knows what they will be able to do with such a large stored database of information. It's a treasure trove and it boggles the mind!

Any such law is likely to cost consumers big money too. As it stands right now, ISPs only have to preserve usage data when asked to do so by law enforcement. Sensenbrenner's proposal would change that to storing usage data on everyone for everything. That's an enormous amount of data and storing it will require a large investment in new hardware and software for ISPs. That alone will result in higher bills for internet access.

The biggest problem with the proposal is that anyone who wants to circumvent it will be able to do so with little or no effort. There are a wide variety of Virtual Private Networks (VPNs) available to consumers; many of them for free. These services redirect internet traffic through a variety of servers around the world and encrypt the data that goes through them. So, the people who are most likely to be hung up by the proposal are honest citizens and small time crooks. Anyone who knows what they are doing is likely to find circumvention of the system a rather simple task.

Another large issue is most Internet Protocol addresses (IP Addresses) are dynamically generated. That means that your

internet address - which is simply a series of numbers - today is likely to be different tomorrow. So your ISP will have to keep track of when each IP address assigned to you was actually in use. If they get your information confused with someone else's, you could find yourself caught up in the middle of a government witch hunt for crimes that you know nothing about! If you think that can't happen, then just consider that there have already been lawsuits over this very issue in a variety of file-sharing cases.

All in all, Sensenbrenner's idea is just another big government power grab designed to infringe on consumer privacy. It is a bad idea that shouldn't ever see the light of day. Given the fact that the electorate sent Republican's back to Congress in the last election to cut the size of government, it is more than a little appalling that the first major piece of information technology legislation being considered in the new congress would significantly expand the scope of government intrusion into the private lives of Americans; endangering their privacy and potentially making them more vulnerable to crimes like identity theft.

byJim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow me on Twitter: