



## Schneier on Security

**Source:** <http://feeds2.feedburner.com/schneier/fulltext>

**Updated:** 11-22

[Update this feed](#)

## **Friday Squid Blogging: New Squid Discovered**

An expedition to study seamounts in the Indian Ocean has discovered some new species, including some squid.

## **Interview with Me**

Yet another interview with me. This one is audio, and was conducted in Rotterdam in October.

## FailBlog on Security

Funny: career fair fail.

## Denial-of-Service Attack Against CALEA

### Interesting:

The researchers say they've found a vulnerability in U.S. law enforcement wiretaps, if only theoretical, that would allow a surveillance target to thwart the authorities by launching what amounts to a denial-of-service (DoS) attack against the connection between the phone company switches and law enforcement.

[...]

The University of Pennsylvania researchers found the flaw after examining the telecommunication industry standard ANSI Standard J-STD-025, which addresses the transmission of wiretapped data from telecom switches to authorities, according to IDG News Service. Under the 1994 Communications Assistance for Law Enforcement Act, or Calea, telecoms are required to design their network architecture to make it easy for authorities to tap calls transmitted over digitally switched phone networks.

But the researchers, who describe their findings in a paper, found that the standard allows for very little bandwidth for the transmission of data about phone calls, which can be overwhelmed in a DoS attack. When a wiretap is enabled, the phone company's switch establishes a 64-Kbps Call Data Channel to send data about the call to law enforcement. That paltry channel can be flooded if a target of the wiretap sends dozens of simultaneous SMS messages or makes numerous VOIP phone calls "without significant degradation of service to the targets' actual traffic."

As a result, the researchers say, law enforcement could lose records of whom a target called and when. The attack could also prevent the content of calls from being accurately monitored or recorded.

The paper. Comments by Matt Blaze, one of the paper's authors.

## A Taxonomy of Social Networking Data

At the Internet Governance Forum in Sharm El Sheikh this week, there was a conversation on social networking data. Someone made the point that there are several different types of data, and it would be useful to separate them. This is my taxonomy of social networking data.

1. **Service data.** Service data is the data you need to give to a social networking site in order to use it. It might include your legal name, your age, and your credit card number.
2. **Disclosed data.** This is what you post on your own pages: blog entries, photographs, messages, comments, and so on.
3. **Entrusted data.** This is what you post on other people's pages. It's basically the same stuff as disclosed data, but the difference is that you don't have control over the data -- someone else does.
4. **Incidental data.** Incidental data is data the other people post about you. Again, it's basically same same stuff as disclosed data, but the difference is that 1) you don't have control over it, and 2) you didn't create it in the first place.
5. **Behavioral data.** This is data that the site collects about your habits by recording what you do and who you do it with.

Different social networking sites give users different rights for each data type. Some are always private, some can be made private, and some are always public. Some can be edited or deleted -- I know one site that allows entrusted data to be edited or deleted within a 24-hour period -- and some cannot. Some can be viewed and some cannot.

And people *should* have different rights with respect to each data type. It's clear that people should be allowed to change and delete their disclosed data. It's less clear what rights they have for their entrusted data. And far less clear for their incidental data. If you post pictures of a party with me in them, can I demand you remove those pictures -- or at least blur out my face? And what about behavioral data? It's often a critical part of a social networking site's business model. We often don't mind if they use it to target advertisements, but are probably less sanguine about them selling it to third parties.

As we continue our conversations about what sorts of fundamental rights people have with respect to their data, this taxonomy will be useful.



**[www.feedbooks.com](http://www.feedbooks.com)**  
Food for the mind