**[Your Data in the Cloud, like it or not!](http://ieeessit.org/2014/02/05/your-data-in-the-cloud-like-it-or-not/)**

Posted on [February 5, 2014](http://ieeessit.org/2014/02/05/your-data-in-the-cloud-like-it-or-not/) by [Jim Isaak](http://ieeessit.org/author/jamesisaak/)

Various suppliers of products & services are now integrating cloud operations as necessary aspects of their offerings.  This has raised questions in an article in Scientific American, “The Curse of the Cloud” (hard copy) and related online entry “[We are Forced to Use Cloud Services](http://www.scientificamerican.com/article/were-forced-to-use-cloud-services-but-at-what-cost/)” about who is in control of your data. Before we disparage this situation, we (technologists) need to consider why it is happening.

From a user perspective, having a “common” file structure between devices can be a real advantage.  My music is there, the files I need for this meeting, when I’m on the road. For those of us using online email services (Gmail, Hotmail, etc.) this is a common concept. Once upon a time (like 3 years ago) I’d email myself a file just so it was stored in the implicit cloud. Google has made that explicit with Google Drive and the aps environment.  And specific services like iTunes/iCloud, Microsoft with Windows 8, Chrome/Android have also been structured to preserve “context” in the cloud that can span multiple systems.  This includes the automated password completion data your browser so kindly provides.  In short, your bank account access is now only as safe as your Gmail or other auto-login product’s protection. Ditto your online health records, etc.

Why?  The technological answer is simple — single devices fail, automate backup. Also for apps that run in the cloud, they can be automatically maintained, less user fuss – more secure. But there is a dark cloud above this silver lining called “vendor lock in”.   Microsoft has constantly been challenged with “how can we sell you another copy of xyz?” (DOS, Word, etc.) Historically this has been accomplished by periodic updates and eventually making an old version obsolete in terms of support, security, file formats, etc. Today the solution is Office 365, where you subscribe to the use of the software, and must connect every 30 days or “lose it”.

“**Your Data Are Ours**” — and of course the data you store in these locations has limited practical portability to a competing environment.  Typically you can export, or “save as” a file in an common format and move it, but with some data files (music) built in DRM may prevent that.  (An interesting example was Amazon’s removal of Orwell’s *1984* from all of the Kindles that had downloaded it when they found they were in violation of copyright. There is some irony in giving Big Brother that capability.)

As the Scientific American article points out, participation in these services is no longer optional. It is the only way to sync your calendar, etc. with the new iOS, and is strongly encouraged by Microsoft Windows 8.  Needless to say, a Chrome book, is marginal “[For those rare times when you aren’t connected to the web](https://support.google.com/chromebook/answer/3214688?hl=en)“.

As you may have noticed, some of these suppliers are also selling or compelled to provide access to your content by the “authorities”. For each country the “authorities” varies, but includes NSA and such.  If you are engaged in a business that spans international boarders, and tries to maintain trade secrets from foreign competitors, you may want to think twice, or even a dozen times, before committing  critical data to the cloud.  Consider the liability of an “innocent” memo stored in the cloud (email, or even just a draft — early draft given version rollback) … that reveals just a bit too much about some key secret.  Back in the last millennium, when lawsuit “discovery” entailed providing access to your file cabinets to an army of paralegals one of them tripped over this comment in one company’s files: “XYZ corp is eating our lunch, we need to buy them out or burn them down” … written prior to the fire that destroyed XYZ corp’s facilities.  Such a cute turn of phrase would be far easier to find with a good search engine and authorized (or even unauthorized) access to your files.

There is a solution which I think might work: buy your cloud services from NSA. Consider this. NSA has the worlds leading experts on cyber-security, and while an obvious target for attack, is probably one of the best defended. They have data centers that can handle the load (if they can ever get the generators in Utah working), and they probably have more restrictions on their abuse of the data than any other entity (with increasing restrictions every day.) — and best of all, they already have a copy (I think I’m kidding here.)

Posted in [Ethics](http://ieeessit.org/category/ethics/), [Future](http://ieeessit.org/category/future/), [Potential Abuse](http://ieeessit.org/category/potential-abuse/), [Privacy](http://ieeessit.org/category/privacy/), [SSITBlog](http://ieeessit.org/category/admin/ssitblog/), [Surveillance](http://ieeessit.org/category/surveillance/) | Tagged [Big Data](http://ieeessit.org/tag/big-data/), [Cloud Computing](http://ieeessit.org/tag/cloud-computing/), [Data Mining](http://ieeessit.org/tag/data-mining/) | [Leave a reply](http://ieeessit.org/2014/02/05/your-data-in-the-cloud-like-it-or-not/#respond)