USA Patriot Act and Cloud Hosting: What you need to know

By Peter Cartier, Fpweb.net, 2012

What's stopping the government from stepping in and seizing your data?

The US PATRIOT ACT 2001 is the product of a Post-9/11 world, a new legislation created to change U.S. policy regarding gathering intelligence for the purpose of preventing further attacks. Deemed a knee-jerk reaction by many and intrusive by others, the unadulterated power and confusion surrounding the Patriot Act have now directly impeded much of U.S. data centers' cloud services.

Many cloud services companies are feeling the sting of companies that are avoiding U.S. governed providers subject to the Patriot Act. This paranoia springs from the risk of their data being swept up in the Act's net if invoked, and as a result they are avoiding U.S. cloud providers as a whole. It is important to note that although it is used as a counter-marketing tool for U.S. data services, such as web hosting companies, similar counter-terrorism laws exist in places like the UK and Canada as well.

The purpose of this article is to outline the basic principles of the Patriot Act, explain how it affects your business, examine how to represent the issue to your clientele and identify the European work in motion to shorten its reach.

What's it all about: The Patriot Act makes any data that is kept by a U.S. company, *both within or outside the U.S. borders*, susceptible to a possible U.S. Government seizure or unwarranted search. A basic example shows that Google and Microsoft, despite having subsidiaries in other countries like Google UK and Microsoft UK, are both U.S. companies and fall under the umbrella of the Patriot Act.

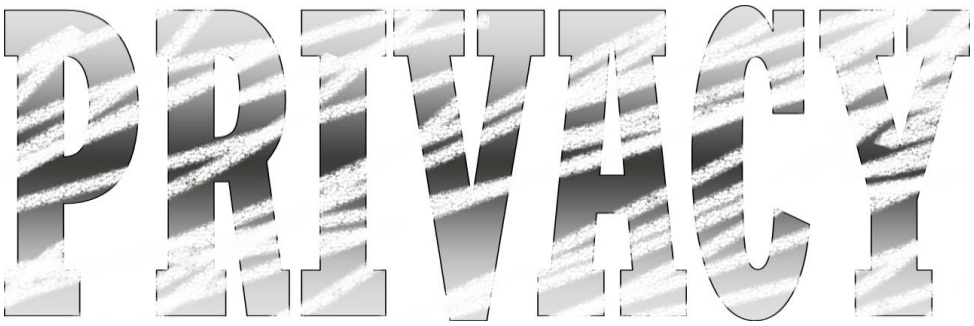
Regardless of where it is stored, any data can be turned over to the government for inspection since the company that is storing the data is governed by U.S. law. Many people and companies already use cloud-based services like Facebook, Twitter, Gmail, Hotmail, etc that, despite where they live, place them within the jurisdiction of the Patriot Act because the cloud providers are all U.S. owned.

Not-so-Safe Harbor: Confusion begins when we consider the Safe Harbor framework - a means for U.S. organizations to comply with the different privacy protection approaches of the EU and Switzerland and ultimately allow data to flow freely between the EU and U.S. The principles of this framework are superseded by the Patriot Act and any data, once it reaches the U.S., can be intercepted with or without a court order depending on the requirements of the data.

Popular opinion: Some people think *(hope)* that a compelling interest must be shown in the data to prove jurisdiction for the request so that it may be granted by the host country's courts. In June of 2011, Microsoft admitted that they cannot guarantee that data won't be handed to U.S. authorities as a result of the Patriot Act saying, "Microsoft cannot provide those guarantees. Neither can any other company." This is the current reality.

Dealing with it: For the time being, every U.S. governed company must comply with the Patriot Act if ever necessary. Businesses would be wise to follow Microsoft's lead in being open to the possibility of this occurring. Explain that your business will always endeavor to be transparent with how each client's data is handled and will always follow any and all applicable laws, including data protection laws. Whenever possible, if you're contacted by law enforcement for any information hosted on your systems, your company will similarly endeavor to redirect law enforcement to the client to give them the opportunity to respond. Explain that you will never replicate a client's data for any outside purpose unless required by law.

Let's look at a scenario of the Patriot Act being invoked and how it may affect innocent customers: A terrorist *(bad guy)* uses a cloud service *(hosting provider)* based in the U.S. to infiltrate or spread propaganda. The FBI tracks the site to the hosting provider. If the threat is significant, the FBI may seize an entire rack of servers for both simplicity and preservation of evidence. As you can imagine, this is how innocent customers may be caught in the net and taken offline.



Most cloud companies, however, aren't quite as expansive as Microsoft or Google and *have that working in their favor*. Private hosting companies, especially ones specific to a certain niche, are at a very low risk of the Patriot Act being exercised for a couple reasons: On one hand, bad guys want a cheap automated service with millions of customers so they can hide *(think GoDaddy or Wordpress).* Secondly, small or private hosting providers get to know their customers and in most cases are industry specific *(think Exchange or SharePoint)* so there's zero chance of a bad guy coming into their network on a cheaper service and jumping over to an Exchange or SharePoint customer's environment. In essence, the Patriot Act, like doing business on the Internet, is *all about minimizing exposure and mitigating risk*.

Your Data Center security: Further information on your data security features is warranted in a continued discussion. Transparency and clarity with the client is always the best way to get your message across. Yes, the Patriot Act affects your company as it does every other, so *as a U.S. based company,* your only move is to keep them informed and offer a dedicated service they can rely on. And tell them what's on the horizon…

The EU Response: Currently the European Parliament is asking for clarification from the European Commission regarding the Patriot Act's reach to their 27 European member states and demanding the obvious: let EU data remain in EU jurisdiction with EU law taking precedence.

A meeting between the European Commission's justice commissioner and German Consumer Protection Minister last November set a deadline of January 2012 to update a 15 year old Data Protection Directive to comply with EU regulations. "We both believe that companies who direct their services to European consumers should be subject to EU data protection laws. Otherwise, they should not be able to do business on our internal market." A draft of this legislation was recently revealed.

While it may take all 27 European member states *several years* to ratify, the new law will certainly help ease tensions surrounding cloud computing security. And with the long shadow cast on U.S. data removed, U.S. governed cloud services will continue business as usual with EU consumers that embrace the cloud *and* their revised EU data protection laws whole-heartedly.

Read Peter Cartier's follow-up articles on the European Commission and Data Protection Laws.

Thanks to Zack Whittaker, a UK journalist, who is credited with exploring the reach of the Patriot Act extensively with his USA Patriot Act series and was first to report Microsoft UK's admittance to being within the reigns of the Patriot Act.