

THE RED BRANCH REPORT

BECAUSE WASHINGTON IS TOO IMPORTANT TO IGNORE

January 2018

OUR VISION

We aim to bring Washington, DC to Silicon Valley.

The large Valley firms have K St. lobbyists, lawyers, and public relations professionals. The small and mid-size start-ups and entrepreneurs have nobody.

We try to fill that gap. This monthly newsletter has “news you can use” that may be important to the IT start-up sector. You may not have the resources to track it, but Washington is too important to ignore.



The US Capitol at dawn

© Red Branch Consulting PLLC 2017

CHINESE RESISTANCE

The slow period that always attends the holiday break in Washington has given us some time to reflect on a larger trend that seems to have gone relatively unnoticed – namely the increasing skepticism and resistance in the West to the incursion of Chinese telecom companies into the American economy.

The phenomenon is not a new one by any means. It goes back at least as far as 2010 when the National Security Agency pressured Sprint to withdraw from a proposed joint venture with Huawei. This was followed, in 2011, by an investigation of Huawei by the House of Representatives Permanent Select Committee on Intelligence. As a result, Huawei does not sell its gear in the US and it's been banned from many joint ventures and purchases. So, in some sense this trend is not at all novel.

“[T]here seems to be a rocky road ahead for the Chinese telecom industry in the US.”

But the atmosphere seems, if anything, to be getting more contentious. Earlier this month, Rep. Mike Conaway (R-TX) introduced a bill (<http://bit.ly/2rghb7z>) that would ban U.S. government agencies from using equipment made by Chinese telecom companies. Under pressure from lawmakers and the Trump Administration, AT&T pulled out of a planned joint venture that would have allowed its customers to purchase Huawei handsets. Lawmakers are also complaining about a request from China Mobile to enter the US mobile market. In addition, American telecoms have an interest in working with the rest of the world (including Chinese companies) to develop technical standards for the next generation 5G network. Those cooperative ventures are also under scrutiny and at risk.

Meanwhile, the Executive Branch continues to exercise its legal authority to block Chinese entry in the US market. Using the powers of CFIUS (the Committee on Foreign Investment in the United States) the U.S. government has blocked a string of Chinese acquisitions over

national security concerns, including, for example, Ant Financial's proposed purchase of U.S. money transfer company MoneyGram International Inc.

Finally, the Senate is likely to take up this year a bill that expands CFIUS (<http://bit.ly/2FPvm6z>). The bill's authors are concerned about recent trends in Chinese investment in the United States, and have described China's approach as "weaponizing" investment to accomplish strategic objectives.

Add to all this the Trump Administration's evident concern about Chinese trade more generally, and there seems to be a rocky road ahead for the Chinese telecom industry in the US. For Valley entrepreneurs that may be a good thing (if they are a competitor) or a bad one (if they are a partner).

Our Prediction: China bashing never gets old. It's something both parties can agree on. And, frankly, it is something that Chinese companies deserve somewhat. Their close ties to the Chinese government are a significant benefit to them in many cases – but when it comes to sales overseas the closeness is a two-edged sword. So look for two things: First, and most obviously, Congress will continue its rhetorical (and perhaps legislative) confrontation with China; Second, and more speculatively, the economic pressures on Chinese companies may grow to such a level that they seek to put some distance between themselves and their government – a move that would put them at odds with national authorities.

AUTONOMOUS VEHICLES

The future of autonomy appears to be now.

The US Department of Transportation has announced a new engagement with the public to develop plans for autonomous vehicles (<http://bit.ly/2D6BJRb>). The Department seeks to support the technology and transportation industry, state and local governments, and other key stakeholders as they consider and design best practices relative to the testing and deployment of automated vehicle technologies.

The requests for assistance cover a range of activities. There is a request for information to help in from defining the technical and policy factors that go into integrating autonomous vehicles into a non-autonomous environment and another on help in removing regulatory barriers to adoption of autonomy.

INTERNET TAXES

Since the early 1990s, the law has been clear – States may only impose taxes on corporations that have "substantial presence" within the State.

In a 1992 case called *Quill v. North Dakota*, the Supreme Court said that a "substantial presence" meant more or less that a company could only be taxed if it had a traditional "bricks and mortar" facility in the taxing state. If it just shipped goods in (say through a mail order catalog) then the State could not impose a sales tax on those goods.

Needless to say, this ruling was a real windfall for the sale of goods on the internet. Most internet retailers have no physical presence in most states, and so the states have long considered the *Quill* ruling a barrier to tax collection. Small, local businesses have, likewise, fought the tax exemption as an unfair advantage for the net. Meanwhile internet sellers have enjoyed a significant benefit.

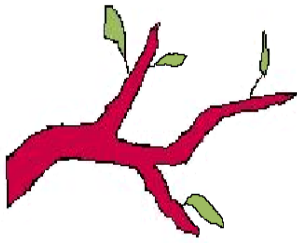
The Supreme Court has just announced that it will reconsider *Quill*. In *South Dakota v. Wayfair*, the court will decide whether it should abrogate the sales-tax-only, physical-presence requirement. Argument in the case will be later this year. A decision will come in June. Best guess: The Court didn't take the case to leave everything unchanged.

Our View: If you have any interest in autonomy (whether in cars or in other devices), now is the time to engage. DOT rules for cars will, almost certainly, be the model for non-automotive autonomy as well.

WASHINGTON TRACKER

Our regular feature – a tracker for legislation and executive action that might be of interest to Valley entrepreneurs. There has been relatively little movement on cyber-related bills, as Congress is taken up with tax reform and other higher priority matters. The major exception is the passage of the 702 reauthorization bill. *Updates and new entries are in italics:*

Bill # or Agency	Title	Description	Status
FCC	Repeal of Net Neutrality Regulations	The FCC considers moves to repeal and/or replace the “net neutrality” regulations adopted by the Commission during the Obama Administration. The revised regulations would permit internet providers to charge variable fees to subscribers based on volume and other factors.	Order adopted by Commission on 14 December 2017. <i>Senate moving to void regulation under the Congressional Review Act. Outcome uncertain.</i> Expect the revision to be immediately challenged in Federal court, where the outcome is also indefinite.
<i>S. 139</i>	<i>FISA Amendments Reauthorization Act</i>	<i>Reauthorizes Section 702 with modest revisions.</i>	<i>Adopted by House; Senate filibuster failed; 702 reauthorization expected to pass this week.</i>
H.R. 387	Email Privacy Act	Amends the Electronic Communications Privacy Act to require a warrant for government access to cloud-stored emails and other electronic content.	Passed Feb. 6 by voice vote in House; awaiting Senate action. Last Congress bill was killed in Senate; possible same result in 115 th Congress.
S. 1691	IoT Cybersecurity Improvement Act	Requires OMB to put security obligations into all Federal IoT procurement contracts; amends CFAA and DMCA to allow white hat security research.	Introduced in Senate August 1 with bipartisan support. Awaiting Senate committee action.
H.R. 1899 S. 823	Protecting Data at the Border Act	Requires border agents to get a search warrant before searching digital devices at the border; currently no warrant is required.	Introduced in House and Senate on April 4; referred to committee; passage unlikely at this time.
H.R. 4036	Active Cyber Defense Certainty Act (ACDC)	Would exempt victims from hacking laws when the aim is to identify the assailant, cut off attacks or retrieve stolen files.	Introduced in House; referred to Judiciary Committee; hearings possible but not certain; no Senate equivalent yet
S. 1693 H.R. 1865	SESTA/FOSTA	Competing bills to prevent the use of open web sites for sex trafficking. Both intend to create liability on the part of site hosts for user content, thus changing the overall structure of Section 230 of the Communications Decency Act	Senate bill passed committee awaiting floor action; House bill passed committee awaiting floor action; challenge of reconciling approaches may delay or prevent passage.



Contact Us

Red Branch Consulting, PLLC

Paul Rosenzweig, Esq.


509 Ct. NE

Washington, DC 20002

O: +1 (202) 547-0660

M: +1 (202) 329-9650

VOIP: +1 (202) 738-1739

 @RosenzweigP

www.lawfareblog.com

www.redbranchconsulting.com

www.paulrosenzweigesq.com

To subscribe or unsubscribe, send an email to: paul.rosenzweig@redbranchconsulting.com

RECOMMENDED READINGS

Internet Chemotherapy (<https://archive.fo/PQAnU>). A hacker hacks the net to save it: “YOU SHOULD WAKE UP TO THE FACT THAT THE INTERNET IS ONLY ONE OR TWO SERIOUS IOT EXPLOITS AWAY FROM BEING SEVERELY DISRUPTED. The damage of such an event is immeasurable given how digitally connected our societies have become, yet CERTs, ISPs and governments are not taking the gravity of the situation seriously enough.” HT: Mark Weatherford

THE LAST WORD

“Most tech companies don’t expect police to regularly raid their offices, but Uber isn’t most companies. The ride-hailing startup’s reputation for flouting local labor laws and taxi rules has made it a favorite target for law enforcement agencies around the world. That’s where this remote system, called Ripley, comes in. From spring 2015 until late 2016, Uber routinely used Ripley to thwart police raids in foreign countries, say three people with knowledge of the system.” -- Uber’s Secret Tool for Keeping Cops in the Dark (<https://bloom.bg/2EMKZdO>).

ProTip: DON’T DO THIS! 😬