THE RED BRANCH REPORT

BECAUSE WASHINGTON IS TOO IMPORTANT TO IGNORE

December 2017

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

YOU SAY SESTA, I SAY FOSTA

Say you run a web service of some sort. Maybe it's a platform for news. Maybe it's a communications system. It really doesn't matter for purposes of this discussion, so long as the service is open to your customers to post their own content.

What responsibility do you have for that content? What if you are a proto-Facebook and one of your users posts a libelous screed falsely accusing a local politician of taking a bribe or if your local news portal has an open comments section where one of your users posts racist pro-slavery rants. Does that impact you?

The question isn't frivolous. Indeed, as this issue goes to press Congress is seized of the question and set to legislate.

> *"Without Section 230 . . . social media could not exist in its current vibrant style"*

The push to regulate speech on the network stems from the unfortunate reality that some websites (most notoriously one known as Backpage) are used by sex traffickers to market their services. Critics of Backpage (and other sites like it) condemn this use of unmitigated internet freedom – and, indeed, it is indefensible, especially when those trafficked into sexual service are children.

In the Senate, a proposal known as SESTA (the Stop Enabling Sex Trafficking Act) aims to render Backpage liable for the injury it causes – but it would do more harm than good.

For years, website service providers were protected by Section 230 of the Communications Decency Act – a provision that, essentially, says that platforms who merely host user generated content generally aren't liable for that content except under federal criminal law.

Without Section 230, for example, social media could not exist in its current vibrant style. A host of nonprofit and community-based online groups, like Wikipedia, could not function as outlets for free expression and knowledge sharing if they were responsible for what

their users posted. Nor, frankly, could any website with an open comment thread.

SESTA changes all that. It would make it easier to prosecute websites who "facilitate" sex trafficking – which means, under the proposal, nothing more than "make it possible." But merely by existing, open websites that host user content are facilitating the publication of that content – that's their very purpose for existence. So, in effect, SESTA would potentially make any online platform liable criminally and civilly if the site were used (even without its knowledge) for sex trafficking.

By contrast, the House proposal (known as FOSTA – the Fighting Online Sex Trafficking Act) gets at the problem directly by criminalizing the use of the web "with the intent" to promote or facilitate prostitution or sexual trafficking. The purpose element is a critical limiting principal that would apply criminal law only to those who act with mens rea (or "bad intent"). And rather than substantively amending Section 230, FOSTA simply (and correctly) makes clear that it doesn't preempt criminal law.

Our Prediction: Something will pass Congress this coming year. FOSTA isn't perfect but it is better than the SESTA alternative. Any Valley entrepreneurs who have an interest in avoiding a content filtering mandate should engage early and often.

VULNERABILITY EQUITIES

The new White House Vulnerability Equities Process is out. (http://bit.ly/2z3rkHT). For the first time, the government has formalized a process for determining whether or not to reveal previously uknown vulnerabilities that it has discovered.

In deciding whether a vulnearbility is to be disclosed, the review board will consider a host of factors, ranging from the scope of the threat (e.g. how widely is the product used?) to the nature of the vulnerability (e.g. is the vulnerablity exploitable remotely or only with physical presence?) and how mitigable the vulnerability is. It will also, on the other side, consider and weigh the operational value to law enforcement or intellgience of maintaing the secrecy of the vulnerability.

Our View: It's good to have a process that is laid out clearly, and it is even better to have a comprehensive list of considerations that will go into the evaluative decision. The problem is the indefiniteness of the determination. While one can certainly acknowledge that this is a multi-factor analysis, public accountability would benefit from some greater sense of how different factors are to be weighed. Don't exepct a lot more disclosures anytime soon.

NET NEUTRALITY

You don't need this report to tell you that the FCC has finally issued adopted its decision on the "repeal" of net neutrality regulations originally promulgated under the Obama administration. You probably also don't need us to tell you how long and tortuous the path has been– including several unsuccessful attempts at regulation before Obama.

But perhaps you may not have had a chance to read the entire proposal, so we did. (http://bit.ly/2jhLQdo). Under existing rules, broadband service providers may not "block" any content; may not "throttle" content by delivering it at differential speeds; and may not allow "paid prioritization" for content based on a differential fee structure.

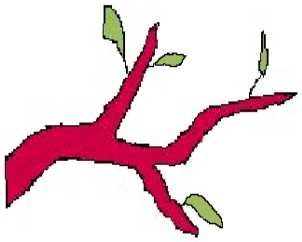
The new proposal from the FCC will, in effect, reverse those rules. The lynchpin of the Obama-era regulations was a determination that broadband providers could be regulated as a public utility. The new Trump FCC rule reverses that determination and classifies broadband providers as an "information service" subject to much less regulation. Likewise, mobile service would be reclassified and the FCC would give up any role in privacy regulation to the FTC.

This is just the start – expect delays in the regulations and a judicial challenge. Our guess: no changes for at least 2 years.

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. *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 Administraiton. The revised regulations would permit internet providers to charge variable fees to subscribers based on volume and other factors.	*Draft of order published in November 2017. Order adopted by Commission on 14 December 2017.* Expect the revision to be immediately challenged in Federal court, where the outcome is indefinite.
H.R. 3989	USA Liberty Act	Modifies secition 702 surveillance authority to require a warrant for certain searches while authorizing some forms of incidental collection and modifying other surveillance authority	Passed the House Judiciary Committee; awaiting House floor action; no equivalent in the Senate yet. *House and Senate will likely act in end of term legislation to continue the program.*
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 115th 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.
S.88 H.R. 686	Developing Innovation and Growing the Internet of Things Act (DIGIT)	Requires FCC to report to Congress on IoT spectrum needs. Requires Commerce to convene working group on IoT to identify federal laws and regulations that inhibit IoT development; and examine how federal agencies can benefit from, use, prepare for, and secure the IoT. Consultation with nongovernmental stakeholders required.	Bipartisan bill introduced January 10 in the Senate; Passed Senate in August. House bill pending in committee. Good candidate for inclusion in larger bill.
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

This report from the Washington Post (http://wapo.st/2j3JwHg) on how President Trump views the Russian interference in the election is a must read: "The feeble American response has registered with the Kremlin. U.S. officials said that a stream of intelligence from sources inside the Russian government indicates that Putin and his lieutenants regard the 2016 "active measures" campaign — as the Russians describe such covert propaganda operations — as a resounding, if incomplete, success."

THE LAST WORD

"The US Supreme Court has agreed to hear arguments in a critical case over data privacy, the outcome of which will likely determine how easily law enforcement can gain access to information stored in tech companies' overseas data centers. Microsoft will go head-to-head with the Justice Department, arguing that the agency cannot use a warrant to collect emails held in Microsoft's Ireland data center." – Gizmodo (http://bit.ly/2AFORzw). Expect a decision in the case before July.