THE RED BRANCH REPORT

BECAUSE WASHINGTON IS TOO IMPORTANT TO IGNORE

October 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

© Red Branch Consulting PLLC 2017

SOURCE CODE REVIEW AND CYBERSECURITY

Hewlett Packard Enterprises (HPE) has allowed the Russian military to review the source code for ArcSight, a cybersecurity alert system. The source code review was a condition required by the Russian government before it would allow Russian business to purchase ArcSight for use in Russian systems. The review was motivated by the facially reasonable-sounding concern the Russians had -- that the American government had not colluded with HPE to put a back door into ArcSight that might be used against the Russians. The problem arises, however, because ArcSight is also widely used in American cybersecurity systems – including systems both in the private sector and in the Pentagon.

> *"The challenge for American businesses that want to do business overseas is clear – there may well be a conflict between their desire to sell to the US government and their desire to market their products overseas."*

The challenge for American businesses that want to do business overseas is clear – there may well be a conflict between their desire to sell to the US government and their desire to market their products overseas.

Consider: ArcSight is for the most part an off-the-shelf technology – so much so that the US government does not, itself, conduct a source code review before installation. Indeed, it would be absurd for the United States to do a code review of all operating systems and applications that it installs within the Federal IT infrastructure – even mission-critical systems like military communications.

By contrast, if the US were to purchase and install a foreign software product it might require such a review. It might even (as in the recent case of Kaspersky security programs) prohibit installation on Federal systems because of concerns about embedded vulnerabilities.

And so, the Russian request was facially reasonable. And yet the review is, legitimately, also cause for governmental concern. What, if any, vulnerabilities in ArcSight may have been disclosed by the

review? And, if discovered in the course of a Russian examination, would the Russians reveal them to HPE? One rather doubts it.

The result is a conundrum. Some may argue that as a condition of selling to the U.S. government, one ought not to be permitted to allow foreign nations to unpack the product. That would, however, have anti-competitive effects of unknown proportions.

By contrast, it may not be unreasonable to require vendors to the Federal government to make a disclosure when they allow a foreign source code review. Especially for a system like ArcSight, which is deeply embedded in US IT infrastructure, that type of disclosure seems both prudent, and probably essential.

Our View: Vendors who market to the US government and overseas need to be sensitive to concerns about the security of the systems they provide. Rumblings on Capitol Hill suggest the possibility of hearings, but greater scrutiny from Federal procurement officers is the more likely result of this disclosure.

FTC REGULTION OF THE IOT TAKES A HIT

Back in January, the FTC brought an action against D-Link, an IoT manufacturer of routers and IP cameras, alleging that D-Link's weak (to be honest, almost non-existent) security was an "unfair business practice." D-Link's products had been implicated in the several botnet attacks and the FTC contended that the weak security put consumer privacy at risk.

In a ruling just last month (http://bit.ly/2y7jYSw) the FTC's enforcement action took a hit. While the FTC's claims of fraud (essentially allegations that D-Link misled consumers about how secure their systems were) can proceed to trial, the District Court threw out the claims based upon the underlying allegations of inadequate security.

Interestingly, the court did *not* say that inadequate security was an inappropriate basis for legal action. Rather, it said that the FTC could not proceed against D-Link unless it was able to identify a concrete harm to consumers – rather than merely speculative supposition.

According to the court: "The FTC does not identify a single incident where a consumer's financial, medical or other sensitive personal information has been assessed, exposed or misused in any way, or whose IP camera has been compromised by unauthorized parties, or who has suffered any harm or even simple annoyance and inconvenience from the alleged security flaws in the DLS devices . . . The absence of any concrete facts makes it just as possible that DLS's

CHINA CRACKS DOWN

China has been heading toward restricting VPNs for some time, but now it is cracking down in earnest with a new cybersecurity law that carries criminal penalties.

Earlier this year, according to a BBC report, Apple informed more than 60 VPNs that they were being removed from the App Store in China on grounds that they were not licensed. Some other apps remain. Apple's chief executive, Tim Cook, said "we would obviously rather not remove the apps" but Apple will "follow the law wherever we do business." Likewise, a Chinese company that operates Amazon's cloud-computing business in China has sent a notice reminding customers to comply with local laws and cease using software such as VPNs that could pierce the Great Firewall.

At the risk of asking a difficult question, Apple's actions do appear to place them in the uncomfortable position of being compliant with Chinese law while resistant to American law enforcement requests (*see* iPhone/San Bernardino/FBI). To be sure the situations are not identical and they are linked by Apple's assessment of business costs and benefits.

But anyone in the business of developing applications and operating systems who wants to do business in China may soon face similar questions.

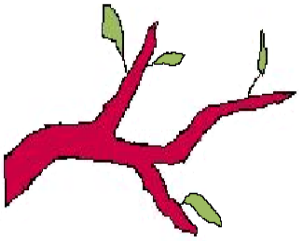
devices are not likely to substantially harm consumers, and the FTC cannot rely on wholly conclusory allegations about potential injury to tilt the balance in its favor."

The story isn't over though – the FTC may be able to restate its unfairness claims, perhaps linking them to the fraud claims. But, at least for now, the mere possibility of consumer harm, without more, will not be enough to form the basis for an FTC enforcement action. For entrepreneurs developing new products, that is probably a welcome development.

WASHINGTON TRACKER

Our regular feature – a tracker for legislation and executive action that might be of interest to Valley entrepreneurs. *Updates and new entries are in italics*:

Bill # or Agency	Title	Description	Status
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	*Introduced by the Chair and Ranking Member of the House Judiciary committee on October 6. Will likely be the base for any further reform efforts.*
H.R. 2481 S. 1157	PATCH Act	Creates Vulnerabilities Equities Review Board to review decision on disclosure of vulnerabilities discovered by USG agencies to vendors.	Introduced May 17 in House and Senate and referred to committees; hearings may occur this year; passage unlikely.
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. 536	Cybersecurity Disclosure Act	Requires corporate Boards to disclose whether they have one member with cybersecurity expertise and steps they are taking to recruit expertise to the Board.	Introduced in the Senate and referred to committee. *Hearing held in September.* Unlikely to pass in current form.
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.



RECOMMENDED READINGS

If you are in business, you need to read the outline of the Trump Tax Plan (http://bit.ly/1X6tAzL). Large companies with overseas cash get a huge break. All corporations get a 15% tax rate. A new business tax rate within the personal income tax code will reduce taxes for small businesses. Some important investment deductions may be eliminated.

Will tax reform pass? Who knows (though we bet against it)? If it does, however, everyone will be effected.

THE LAST WORD

According to Politico (http://politi.co/2ww6BYg), "[t]he IRS will pay Equifax $7.25 million to verify taxpayer identities and help prevent fraud under a no-bid contract issued [September 30], even as lawmakers lash the embattled company about a massive security breach that exposed personal information of as many as 145.5 million Americans."

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