THE RED BRANCH REPORT

BECAUSE WASHINGTON IS TOO IMPORTANT TO IGNORE

September 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

IMPROVING IOT CYBERSECURITY

Just before Congress went out for the August recess, Senator Mark Warner (D-VA) and a bipartisan group of three other Senators, introduced S. 1691, the IoT Cybersecurity Improvement Act of 2017. The bill attempts to use the purchasing power of the Federal government as a lever to drive increased cybersecurity standards for internet-connected devices. This is a relatively common Federal tactic where it sets standards for a product that it purchases in bulk quantity, hoping (and expecting) that its intervention in the market as a purchaser will drive necessary change without resorting to more formal regulation. Under this bill, all Federal IoT purchase contracts would be required to have a series of new contractual clauses mandating a suite of security improvements.

"The bill attempts to use the purchasing power of the Federal government as a lever to drive increased cybersecurity standards for internet-connected devices."

Most notable of these new contractual obligations would be a requirement that vendors certify that the "hardware, firmware or software" in a device contains no known security vulnerabilities; can accept authenticated updates; uses current industry-standard protocols for communications, encryption and interconnection with other devices; and has security mechanisms for remote administration of the device that can themselves be updated in response to threats and breaches.

Certification is a significant obligation – false certification is criminal and mistaken certification can lead to contractual oblivion. Under this provision, there would be no room for legacy vulnerabilities, unpatchable systems, or the use of out-of-date standards. Gone will be the days of fixed passwords. If widely adopted, these requirements would transform IoT manufacturing in ways that are difficult to overestimate. Today's IoT devices often have known bugs, are sometimes unpatchable, and typically do not use the most up-to-date security standards.

The reason for this is simple – implementing those requirements costs money and delays a device's time to market. Today the IoT market is characterized (much as software development was many years ago) as "market now; fix later (or never)."

The bill has several other provisions, the most notable of which is a safe harbor amendment to the Computer Fraud and Abuse Act and Digital Millennium Copyright Act to limit criminal penalties against white hat researchers who, "in good faith," are testing the cybersecurity of the devices being sold to the government. The good faith test will, ultimately, be derived from Federal (yet-to-be-developed) guidelines on vulnerability disclosure.

One question we have that the bill doesn't answer: Why is it necessary? Presumably OMB could adopt the procurement standards without a law. That makes clear that the only critical legislative portion of the bill is the CFAA/DMCA amendments.

Our Prediction: This bill won't become law this year. [Heck, nothing will ...]. OMB will, however, begin to adopt some of the certification standards as part of Federal procurement contracts. It will be a half-dozen years, however, before there are significant impacts on IoT security.

REFLECTIONS ON THE GOOGLE AFFAIR

By far the most interesting thing that happened over the summer break was the controversy that erupted at Google. For those who live on the North Pole, the short version is this: A Google engineer, James Damore, published a note questioning Google's efforts to diversify its workforce, most notably in its efforts to recruit women. The resulting uproar was both unsurprising and fierce and he was soon fired. He has now sued for a violation of his own civil rights.

I have absolutely no interest in wading into the "debate" such as it is, over diversity in the Valley. I imagine that all of those reading this Report have far more well-informed opinions about the issue than I do. It is, however, worth considering some of the lessons that tech companies might take from the episode.

Some are obvious: Employees really do not have unfettered rights of free speech within the company. Others are less obvious: when Y Combinator starts a black list of sexual harassment by venture capitalists, it is only a short step from there to a black list of tech start-ups.

But the least obvious lesson, I think, is that in Washington everything counts. I am completely confident in making an off-the-wall prediction:

ELECTORAL SECURITY

Senators Amy Klobuchar (D-MN) and Lindsey Graham (R-SC), have proposed an amendment (SA 656) to this year's National Defense Authorization Act. The NDAA is set to be considered by the Senate during this month.

The proposed amendment is modest in its terms (no doubt because securing bipartisan agreement on any aggressive electoral reforms would be nigh on impossible). In summary, it does the following:

* Tasks DHS and the Electoral Assistance Commission with developing a set of "best practices" for the cybersecurity of the electoral infrastructure; and

* Authorizes Election Technology Improvement grants to the States to be used to address identified risks and vulnerabilities and to purchase new and/or upgrade older election system hardware.

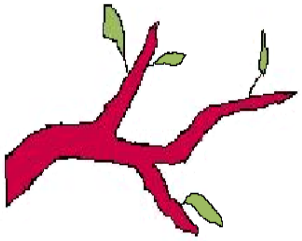
While it is hard (indeed almost impossible) to object to any of the purposes behind the Klobuchar/Graham proposal, it is depressing, indeed, to see that so little is legislatively possible. A set of best practices and a promise to throw money at the problem is the barest of starts on a difficult problem. And, one suspects, in these times of fiscal restraint, even the promise of money may not be realistic.

sometime reasonably soon, someone in Washington will take it into their head to "fix" the gender disparity problem in the Valley. I can't tell you that it will be a legislator. It may be some executive branch official. But you can bank it – unless the tech community takes aggressive steps soon, there will be hearings in Washington. And after that ... who knows?

WASHINGTON TRACKER

Our regular feature – a tracker for legislation and executive action that might be of interest to Valley entrepreneurs. Nothing happened during the August recess, so this is a *status quo* report:

Bill # or Agency	Title	Description	Status
FCC	Repeal of Net Neutrality Regulations	The FCC has begun the process of considering how 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.	With the change in Administration, the revised regulations are very likely to be adopted by the Commission sometime before the end of this year. Expect the revision to be immediately challenged in Federal court, where the outcome is indefinite.
H.R. 2841 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. 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; Reported to the Senate June 10 without dissent. House bill pending in committee. Good candidate for inclusion in larger bill.



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

Ben Buchanan, "Nobody But Us," Hoover Institution. (http://hvr.co/2woV13e). The United States and its partners have relied on an approach sometimes called Nobody But Us, or NOBUS: target communications mechanisms using unique methods accessible only to the United States. Its success depends on a number of American advantages that are under serious threat. The decline of these advantages renews the tension between offense and defense signals intelligence.

THE LAST WORD

Per Eric Geller (of *PoliticoPro*): "Trump has yet to appoint people to the government's top two IT posts [the Federal CIO and CISO], or to the top two leadership posts at the Department of Homeland Securit's cyber division. At the State Department, a high-level cyber diplomacy pot sits vacant. . . . . And he has not yet named a director of the technical standards agency NIST, which writes the digital security guidelines that the government — and many in the private sector — rely on to protect data." [Note, however, that in late August, President Trump did nominate John Demers to be Assistant Attorney General for the National Security Division – with cybersecurity prosecution responsibilities.]