THE RED BRANCH REPORT

BECAUSE WASHINGTON IS TOO IMPORTANT TO IGNORE

May 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

BUILD A BETTER MOUSETRAP

Herewith some speculation – worth more or less exactly what you are paying for it. 😊

Recall that several weeks ago the Department of Homeland Security instituted a laptop/tablet ban on flights from ten designated airports in the Middle East. While some speculated that the ban was intended as an economic measure to protect American airlines, there is good reason to believe that the real impetus behind the ban was a change in the available threat intelligence about potential terrorist activity. In other words, DHS (based on information derived from intelligence sources) came to believe that terrorist actors were making a renewed (and improved) effort to put undetectable explosives into laptops and tablets. [We don't worry about smart phones because the casing is so small that they wouldn't contain enough explosive to damage a plane.]

If that assessment is correct, then there is a certain lack of logic to the DHS ban. After all, there is no reason to think that the terrorists will limit their attacks to direct flights from the Middle East. Nothing would prevent a determined adversary from first travelling to somewhere in Europe (with a laptop in checked baggage) and then removing it to use in transit to America. Nor is there any logical barrier to taking a laptop out of checked baggage upon arrival in the U.S., and using it on a connecting domestic flight. If the intelligence is serious (and there is no reason at this juncture to doubt it) then the electronics ban will likely be expanded – and public reports suggest that an expansion to European flights may occur soon. As we said, this is speculation. But it makes sense from a security standpoint (though not from a public relations standpoint – the response to a broader ban will be severe) and Secretary Kelly has hinted at this prospect in recent public remarks.

> *"There is no reason to think that the terrorists will limit their attacks to direct flights from the Middle East."*

And that, in turn, is an opportunity for hardware manufacturers. Today, the problem for the U.S. government is that it cannot be sure that the innards of a device are explosive-free. Device manufacturers cannot fix the detection problem. But they can (and should) think hard about alternatives. For example, is there a way to manufacture the casing of a device such that it is tamper-evident? Can we build a device where one can detect that it has been opened? Alternatively, is there a way to make devices readily openable, so that the interior can be visually inspected prior to boarding? If so, can you do it in a way that preserves the integrity of the components and won't void the warranty?

I'm no engineer, so the feasibility of these solutions (or others not identified) is beyond my expertise. It does seem, however, as though the demand for such products is likely to grow in the near future and hardware entrepreneurs should be making plans now.

LOSING TALENT TO NEW ZEALAND?

Will developer talent be moving to New Zealand? Perhaps so, as the New York Times reports:

"A municipal program to fly in 100 developers [during May] — wine them, dine them and offer them jobs — was expected to draw 2,500 applications. But the recruitment effort, called *LookSee Wellington*, was besieged with more than 48,000 entries, including workers at Google, Amazon, Facebook, M.I.T. and NASA. At one point so many people checked out the program that the website failed.

For all sorts of reasons, New Zealand suddenly makes sense. The cost of living is less than in San Francisco. Commuting is less wearying. And American politics, 'Brexit' and the Islamic State are on the other side of the world."

THE AMERICAN TECHNOLOGY COUNCIL

On May 1, the Trump Administration issued an Executive Order (http://bit.ly/2oPE3cs) establishing the American Technology Council. The Council was established "to promote the secure, efficient, and economical use of information technology to achieve [the Government's] missions. . . . To effectuate this policy, the Federal Government must transform and modernize its information technology and how it uses and delivers digital services."

The new Council will include representatives from almost every relevant Federal agency and, perhaps most notably, will include in its membership, the Senior Advisor to the President, Jared Kushner. The formal tasking of the council is to "coordinate the vision, strategy, and direction for the Federal Government's use of information technology and the delivery of services through information technology." In short, this is an effort to centralize at the White House level transformative IT efforts of exactly the sort being developed by US Digital Services, and GSA's component 18F. [We wrote about the GSA Inspector General's audit of 18F in the March 2017 issue of The Red Branch Report.]

Our assessment: Rumor has it that the cybersecurity executive order (which was just issued late last week, and which we will review in a forthcoming issue -- http://bit.ly/2pp97Qf) was held up, in large part, because of the desire to carve out IT innovation for a separate effort to be led by Mr. Kushner. In many ways, the new ATC is promising – after all, when the President's most trusted senior advisor is assigned a tasking, that signals its importance. Silicon Valley entrepreneurs can anticipate an increased emphasis on disruptive technology – look for new seed money funding programs; cooperative public—private ventures; and greater opportunities to sell into the Federal market.

WASHINGTON TRACKER

Our regular features – a tracker for legislation and executive action that might be of interest to Valley entrepreneurs:

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.
DHS	Privacy Policy Guidance 2017-01	In 2007, DHS promised that all of the data that it held in "mixed systems" (that is systems that contained personal information about both Americans and non-Americans) would be protected by the Privacy Act. This new guidance, implementing a decision of the Trump Administration, rescinds that decision. The personal information of non-Americans collected by DHS will no longer be protected under the umbrella of the Privacy Act.	Implemented with immediate effect on April 27, 2017. Practical impact uncertain at this time.
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.
H.R. 1530	Financial Transparency Act	Significant open data initiative that would direct the government's eight financial regulatory agencies to adopt data standards for the information they collect from the private sector in order to reduce duplication, burden and fraud and make it available for download, accessible via application programming interfaces and easily searchable.	Introduced in House; hoped for introduction of Senate version ahead; in last Congress initiative languished but this has better prospects as OMB Director Mulvaney may be supportive
S. 770	MAIN STREET Cybersecurity Act	Would require NIST to take into account needs of small businesses in setting NIST cybersecurity framework standards.	Introduced in Senate March 29 with bipartisan support. Unlikely to pass independently; may get added to larger bill.
H.R. 1899/ S. 823	Protecting Data at the Border Act	Would require 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.

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
@RosenzweigP
www.lawfareblog.com
www.redbranchconsulting.com
www.paulrosenzweigesq.com

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

RECOMMENDED READINGS

Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," (CNA, March 2017), https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf.

THE LAST WORD

Last month we reported on the possibility that the Trump Administration would significantly modify the H1-B visa program. That seems to be a bullet that the tech community has successfully dodged, at least for now.

On April 18th President Trump issued an Executive Order (http://bit.ly/2pB59U1) on hiring Americans. With respect to the H1-B program, all the Order did was require Federal agencies to "suggest reforms to help ensure that H-1B visas are awarded to the most-skilled or highest-paid petition beneficiaries." Hardly the ban we were fearing.