THE RED BRANCH REPORT

BECAUSE WASHINGTON IS TOO IMPORTANT TO IGNORE

April 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

WILL THE FEDS REGULATE INTERNET OF THINGS SECURITY?

The Federal Trade Commission (FTC) has, over the past five years, greatly increased its regulation of cybersecurity matters under the guise of its authority to protect consumers. One famous case, involving Wyndham Hotels, established the legal principle that the FTC could challenge inadequate security measures as an "unfair business practice" and impose civil fines on those who had acted without reasonable regard for basic cybersecurity requirements.

That trend provides the context for a likely source of significant regulation over the next few years: the FTC's possible response to the exposure of systematic vulnerabilities in some of the components that make up the Internet of Things. No doubt readers are familiar with the Mirai botnet attacks in late 2016 that temporarily disabled a significant portion of the network. Those attacks were staged through IoT devices – routers, DVRs, and cameras – that had little or no basic security. Will the FTC now step in and regulate IoT security standards?

> *"the threat of government regulation will drive standardization and adoption of a security requirement."*

Those opposed to a Federal regulatory mandate (or, more gently, Federal standard-setting) argue that the IoT industry can self-regulate and that the imposition of requirements or standards will stifle innovation and increase costs. They contend that the security problems for IoT devices are too diverse and complex to be suitable for Federal control and that the free market will solve the problem through traditional pricing and liability mechanisms.

On the other side of the ledger, all acknowledge that the legacy IoT security issue is massive. Because self-regulation may not produce adequate security and IoT devices are already deeply embedded in all aspects of our personal lives and commerce, the argument for some form of Federal intervention is akin to that which drove food safety

requirements a century ago: This is simply an area where the free market fails and we cannot afford the costs of repair when the scale of IoT insecurity is realized.

Perhaps surprisingly, for the moment the FTC seems to be holding fire. Last month, the acting head of the FTC, Maureen Ohlhausen, said that she did not see any harm to consumers from the lack of security standardization and that she believes that the IoT industry should largely be left to regulate itself, rather than being subjected to external oversight.

Our Prediction: It won't last. After the next Krebs/Dyn attack, calls for regulation will increase. Much as happened with point-of-sale security, the threat of government regulation will drive standardization and adoption of a security requirement. Best guess at a timeline: 2-3 years.

Our Recommendation: The FTC is ill-equipped for this task. If you agree that some regulatory effort is inevitable, perhaps consider whether there is a better alternative venue – NIST?

THE H1-B IMPLOSION

We usually don't think of immigration law as a direct impact on tech development. The Trump Administration will change that.

Many Silicon Valley employers bring in talented software engineers through a visa program known as H1-B. Large employers rely on the program for outsourcing their engineering requirements. Smaller start-ups often use the H1-B visa to find critical talent.

The H-1B program, authorized by the 1965 Immigration and Nationality Act, permits high-skilled foreigners to take jobs in "specialty occupations" including biotechnology, engineering, and physical sciences. Visas last for three years, with the possibility of extending to six years. The program is capped at 85,000 visas per year for commercial enterprises, and the application quota is typically filled within 3-5 days of being opened. Every year tech start-ups and large tech companies (Google, Facebook, IBM) take advantage of these provisions to hire foreign engineering talent.

The first step in the Trump H1-B crackdown was to suspend a practice known as "premium processing." This was a program that allowed for expedited H1-B applications. Without expedited processing, the decision time frame for an H1-B applicant can be months, instead of weeks – so, now just imagine that you have to wait 6 months for the engineer you need to be cleared for work.

With the purpose of "protecting American workers" from outsourcing, a draft executive order that is circulating would further constrain the H1-B program. It is likely that the revised H1-B program would have fewer slots available and even more stringent requirements for proving the unavailability of equivalent American employees.

Our prediction: The Trump Executive Order will generate significant push-back from Silicon Valley but will, in the end, result in a reduction in H1-B visas on the ground. This will result in many companies transitioning

FROM UP CLOSE TO THE ICE

It isn't just the United States that feels threatened by the cyber-insecurity of its critical infrastructure. This is from the 2017 Threat Assessment by the Norwegian Police Security Service:

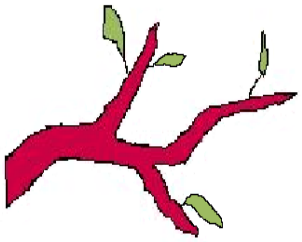
"Norwegian critical infrastructure will continue to be targeted by foreign intelligence activity in 2017. The aim of such intelligence operations is to collect information about the infrastructure concerned and to prepare for data manipulation or sabotage in the event of a tense foreign or security policy situation. Power supply systems and electronic communications services are critical infrastructure that is especially likely to be targeted by intelligence activity."

some, or all, of their work to non-American sites. For larger companies that may be feasible; for Valley entrepreneurs, less so. In 2013, the Immigration and Citizenship Office of Canada posted billboards along the San Francisco highways ("H-1B Problems? Pivot to Canada!"). Back then, it was a bit of a joke –now it may become reality.

WASHINGTON TRACKER

Our regular features – a tracker for legislation and executive action that might be of interest to Valley entrepreneurs. It's still early days in the legislative and executive calender so most of these are speculative:

Bill # or Agency	Title	Description	Status
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
New York State Rule	Cybersecurity Requirements for Financial Services Companies	Financial industry in NY must have a cyber-security plan in place, including, e.g,. network penetration testing, establishing cyber audit trails, and restricting access to customer data. Firms must also have a senior security officer and submit an annual compliance certificate.	New rule adopted in March 2017. Rule is limited to one State and one industry sector. We predict that the requirements will become standard in many sectors and many states and also become *de facto* negligence standard for cyber actors
S.J. Res.34	Resolution of Disapproval	Repeals Obama-era Federal Communications Commission regulations that required internet service providers to get their customers' permission before using their data for advertising.	Signed into law April 3, 2017 – Public Law 115-22
FCC	Office of Economics and Data (OED)	Creation of new office at FCC to provide economic advice to FCC on improving management of data, reports and analysis; and taking a long-term approach to the FCC's policy on emerging issues, like the internet of things and increasingly dense wireless networks.	Office opened April 2017. Will likely have significant market-based approach influence on FCC actions.
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.



RECOMMENDED READINGS

Natasha Cohen, "The Evolving Cybersecurity Regulatory Environment: Tracking Current Trends and Staying Ahead of the Curve," Columbia Journal of International Affairs, https://jia.sipa.columbia.edu/online-articles/evolving-cybersecurity-regulatory-environment -- useful summary of regulatory trends in assessment, audit, and liability.

THE LAST WORD

According to Alex Karp, the CEO of Palantir, "the Valley is marching off a political cliff." His reasoning is simple: Valley executives are "overplaying" their hand against President Trump. Karp cites opposition to the immigration executive order as exhibit A in his argument that the tech industry stands in stark opposition to the President.

Perhaps so. This Report is nonpartisan – though my views are pretty easy to discern – so I would never urge anyone to withhold their opinion on issues of public import. Nonetheless, the reality is that Washington is not only too important to ignore, it may also be too important to anger. One can easily see President Trump responding to tech-entrpreneur opposition to his policies by, for example, attempting to subject off-shore profits to taxes. And, while job losses today are being blamed on immigration, it is a short step to blaming technological innovation.

All of which is a long way of saying that politics is a blood sport. If you get in the game, you'd better be prepared for a contest.

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