

THE RED BRANCH REPORT

BECAUSE WASHINGTON IS TOO IMPORTANT TO IGNORE

November 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

DATA SCRAPING AND THE PUBLIC SQUARE

HiQ is a startup data analytic company that uses big data to improve employer human resource services. Combining the work of data engineers and human resource experts, the company aspires to help its customers retain talent. As they put it “why do recruiters know more about your employees than you do?”

To answer that question HiQ ingests data, much of it scraped from public facing web sites. One of the most salient sources of information is LinkedIn, the professional networking company owned by Microsoft. Since LinkedIn is, fundamentally, about employee mobility, it is a rich source of data about the phenomenon. Or, to put it more bluntly, since employees use LinkedIn to find new jobs, HiQ is in the business of figuring that out and helping the current employer retain its talent.

“Social media are, in effect, the new public square. Do the platforms that create social media have any public obligation as a result?”

Companies with public facing websites that host consumer data, like LinkedIn, Twitter, Facebook and most any other social media platform, often object to this public scraping phenomenon. Sometimes the objection is couched in terms of a public good, as the companies profess to be protecting their users’ privacy. More prosaically, since the platform often charges license fees or access fees of some sort to larger quantities of data collected as part of their business model, they view public scraping as a business threat. After all, LinkedIn charges recruiters, salespeople and job hunters for higher levels of access to profile data. Why would the welcome HiQ monetizing that same access?

In 2016, the Ninth Circuit faced the same issue in a suit brought by Facebook against Power Ventures (<http://bit.ly/29L4wzt>). That court concluded (wrongly, in our judgment) that scraping a public web site was a violation of the Computer Fraud and Abuse Act (CFAA) because Power Ventures had received a “cease and desist” letter from Facebook and continued its scraping practice anyway.

Relying on that precedent LinkedIn did the same thing with respect to HiQ. They sent a cease and desist letter. HiQ persisted and the matter went to court. And, oddly enough, HiQ won in the district court. Despite the Power Ventures precedent, the district court order LinkedIn to permit HiQ to continue its scraping activities. The dispute is now on appeal to the Ninth Circuit.

The case raises a number of issues critical to Silicon Valley: First, and foremost, it will define what is, and is not, an acceptable data analytic business model. If “data is the new oil” then who controls access to the oil is a critical business question. Second, and of equal significance, the case may help define what constitutes a violation of the CFAA – is it a crime to access a public web site just because the owner told you not to, but didn’t stop you with any technical means? And finally, the case asks big philosophical questions about free speech. Social media are, in effect, the new public square. Do the platforms that create social media have any public obligations as a result?

Our Prediction: Nobody ever made any money predicting court cases, but our guess is that the Ninth Circuit will follow its own precedent and rule for LinkedIn. After that the Supreme Court will be asked to review the case, but we are guessing they will duck the issue, because they don’t understand it.

HACKING THE IOT – VARSITY DIVISION

This newsletter has often given attention to the security and privacy risks associated with the proliferation of consumer device that are enabled in some way for communications across the network. This month, our interest in the matter took a sizeable leap forward, thanks to the work of the DHS Science & Technology division.

At the CyberSat summit in Virginia earlier this month, the aviation testers in S&T reported that they had succeeded in remotely hacking into the control systems of a Boeing 757 (<http://bit.ly/2zI8PI6>). To be fair, the intrusion took place under test conditions, without significant active defense measures being employed and in an artificial environment.

Still, as a proof-of-concept effort the intrusion is a cautionary tale. DHS employees accessed the aircraft's systems via radio frequency communications. The test is classified and the details of the hack have not been disclosed. But DHS has said that access was attained using gear that was “typical stuff that could get through security.”

Food for thought next time you fly across country.

ACDC

Fans of the rock group ACDC may soon have a cybersecurity bill named after the band. The Active Cyber Defense Certainty Act (or “ACDC”) was introduced by Rep. Tom Graves (R-GA) in mid-October and referred to the Judiciary Committee for consideration.

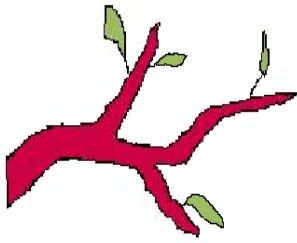
The bill would do two distinct things: First it would prohibit the prosecution of individuals who are victims of a cyber intrusion and use active cyber defense measures to attribute the attack; to disrupt the attack or, in effect, to develop intelligence about the attacker for the prevention of future attacks. Explicitly prohibited are more intrusive forms of “hack back” including any act that would “recklessly” cause injury or purposefully destroy data other than the victims’ own data. Prosecutorial forbearance will also be contingent on notification by the victim to the FBI of an intent to respond.

Second, and more creatively, the bill would also allow victims to voluntarily provide preemptive notification of tools to the FBI -- i.e. “this is what I plan to use” in response to an attack.” This would put the FBI in the exceedingly unusual position of providing a technical review for which it may lack the qualifications and, even more oddly, of approving an otherwise criminal act before it takes place and in a sense “blessing” the violation.

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
H.R. 3989	USA Liberty Act	Modifies section 702 surveillance authority to require a warrant for certain searches while authorizing some forms of incidental collection and modifying other surveillance authority	<i>Passed the House Judiciary Committee; awaiting House floor action; no equivalent in the Senate yet</i>
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 115 th 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.
<i>H.R. 4036</i>	<i>Active Cyber Defense Certainty Act (ACDC)</i>	<i>Would exempt victims from hacking laws when the aim is to identify the assailant, cut off attacks or retrieve stolen files.</i>	<i>Introduced in House; referred to Judiciary Committee; hearings possible but not certain; no Senate equivalent yet</i>



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

The new White House Vulnerability Equities Process is out. (<http://bit.ly/2z3rkHT>). We'll have more analysis next month.

Meanwhile, we recommend: Reaper: The Calm Before the IoT Storm (<http://bit.ly/2z41qmY>) – “experts are sounding the alarm about the emergence of what appears to be a far more powerful strain of IoT attack malware – variously named “Reaper” and “IoTroop” – that spreads via security holes in IoT software and hardware. And there are indications that over a million organizations may be affected already. Reaper isn’t attacking anyone yet. For the moment it is apparently content to gather gloom to itself from the darkest reaches of the Internet. But if history is any teacher, we are likely enjoying a period of false calm before another humbling IoT attack wave breaks.”

THE LAST WORD

On a personal note, I wanted to take this opportunity to let you know that, effective November 20, I have taken a position as a Senior Fellow at the R Street Institute (<http://www.rstreet.org/>). I will continue my consulting practice through Red Branch, but I look forward to the chance to work with the Tech and National Security policy wonks at R Street on broader public policy issues of interest to the tech community.